## ОТРАСЛЕВАЯ И РЕГИОНАЛЬНАЯ ЭКОНОМИКА

**А. А. Моросанова**[1]
МГУ имени М. В. Ломоносова / РАНХиГС (Москва, Россия)

УДК: 334.02; 338.23
doi: 10.55959/MSU0130-0105-6-60-3-8

# БОЛЬШИЕ, ПЕРСОНАЛЬНЫЕ, ОБЕЗЛИЧЕННЫЕ ДАННЫЕ: ПРОБЛЕМЫ ОТРАСЛЕВОГО РЕГУЛИРОВАНИЯ[2]

*Развитие цифровой экономики в России сталкивается с противоречием между необходимостью свободного обмена большими данными и усилением контроля за персональными данными. Введение национального проекта «Экономика данных» и новых федеральных законов о персональных и деперсонализированных данных обострило проблемы правового регулирования этой сферы. Исследование направлено на выявление экономических проблем в области больших данных, возникающих из-за регуляторных пробелов и новых норм защиты персональной информации. Методологической основой выступает новая институциональная теория, в частности теория управления трансакциями О. Уильямсона. В статье применяются методы сравнительного институционального анализа и экономико-математического моделирования для оценки эффективности штрафных санкций. Установлены различия в специфичности больших и персональных данных как ресурсов, что обосновывает необходимость дифференцированного регуляторного подхода. Выявлены структурные альтернативы регулирования: от полного государственного контроля до рыночных механизмов с промежуточными гибридными формами. Основными препятствиями развития рынка больших данных являются неопределенность статуса обезличенных данных и отсутствие надежных методов деперсонализации. Моделирование показало, что введение оборотных штрафов создает чрезмерную нагрузку на малые и средние предприятия, предварительно инвестировавшие в кибербезопасность. Обеспечение развития цифровых отраслей требует обязательного государственно-частного партнерства в нормотворчестве через саморегулируемые организации, учитывающего высокую скорость технологических изменений.*

**Ключевые слова:** большие данные, персональные данные, обезличенные данные, деперсонализация, специфичность, защита информации, утечки, цифровая экономика.

[1] Моросанова Анастасия Андреевна — к.э.н., научный сотрудник, Экономический факультет, МГУ имени М. В. Ломоносова, Центр исследований конкуренции и экономического регулирования ИПЭИ РАНХиГС; e-mail: aamorosanova@gmail.com, ORCID: 0000-0002-2418-6706.

[2] Статья подготовлена в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС.

Цитировать статью: Моросанова, А. А. (2025). Большие, персональные, обезличенные данные: проблемы отраслевого регулирования. *Вестник Московского университета. Серия 6. Экономика,* 60*(3),* 172–193. https://doi.org/10.55959/MSU0130-0105-6-60-3-8.

**A. A. Morosanova**
Lomonosov Moscow State University / RANEPA (Moscow, Russia)
JEL: L86, L51

# BIG, PERSONAL, DEPERSONALIZED DATA: PROBLEMS OF INDUSTRY REGULATION[3]

*The development of Russia's digital economy faces a contradiction between the need for free big data exchange and increasing control over personal data. The introduction of «Data Economy» national project and new federal laws on personal and depersonalized data has intensified regulatory problems in this sphere. The research aims to identify economic problems in big data field arising from regulatory gaps and new personal information protection norms. The methodological foundation is new institutional theory, particularly O. Williamson's transaction cost economics. The author applies comparative institutional analysis and economic-mathematical modeling methods to assess the effectiveness of penalty sanctions. Differences in the specificity of big data and personal data as resources were established, justifying the need for a differentiated regulatory approach. Structural regulatory alternatives were identified: from complete state control to market mechanisms with intermediate hybrid forms. The main obstacles to big data market development are uncertainty regarding anonymized data status and the absence of reliable depersonalization methods. Modeling showed that introducing turnover-based fines creates excessive burden on small and medium-sized enterprises that previously invested in cybersecurity. Ensuring digital industry development requires mandatory public-private partnership in rulemaking through self-regulatory organizations that account for a high pace of technological changes.*

**Keywords:** big data, personal data, depersonalized data, depersonalization, information protection, leaks, digital economy.

To cite this document: Morosanova, A. A. (2025). Big, personal, depersonalized data: problems of industry regulation. *Lomonosov Economics Journal*, 60*(3),* 172–193. https://doi.org/10.55959/MSU0130-0105-6-60-3-8

## Введение

В 2025 г. вступил в силу новый национальный проект «Экономика данных», который пришел на смену проекта «Цифровая экономика». Акцент, очевидно, смещается на определенные сквозные технологии — искусственный интеллект, нейросети и большие данные, что означает

[3] The article was written on the basis of the RANEPA state assignment research programme

повышенную заинтересованность в развитии этих областей со стороны государства, в том числе и в установлении новых мер поддержки и регулирования. О необходимости введения нормативных актов, специфицирующих отношения по поводу больших данных, свидетельствуют следующие факторы:

- неразвитость рынка больших данных, преобладание «серых» практик обмена данными между компаниями и брокерами данных;
- наличие правовых противоречий и «пробелов» в существующих правовых нормах (Осипов и др., 2020), а также их различных трактовок судебными органами;
- возрастающая роль цифровых экосистем и платформ, потенциально выступающих «привратниками» на рынках, что может приводить к превалированию мезоинститутов (Шаститко и др., 2023) над государственными (и даже надгосударственными) институтами.

На данный момент сфера больших данных не имеет специфического регулирования (в последние 6 лет было принято 9 ГОСТов, которые являются необязательными к выполнению), исключение составляет та область, которая касается персональных данных. После ряда крупных утечек персональных данных с 2022 года были приняты шаги по усилению контроля за персональными данными и стимулированию компаний к применению необходимых мер кибербезопасности. Был принят Федеральный закон от 30.11.2024 № 420-ФЗ (Федеральный закон, 2024, 30 ноября), усиливающий ответственность за нарушение должного обращения с персональными данными, в том числе предполагающий введение оборотных штрафов за повторные утечки. Также принят Федеральный закон от 08.08.2024 № 233-ФЗ (Федеральный закон, 2024, 08 августа) о деперсонализации данных — процессе, который «превращает» персональные данные в обезличенные, которые (при определенных условиях) можно передавать/продавать третьим лицам.

Цель статьи заключается в выявлении особых экономических проблем в сфере больших данных, которые могут быть вызваны как отсутствием определенных регуляторных механизмов, так и новыми нормами в сфере персональных данных. На основании различия в специфичности ресурсов больших и персональных данных (раздел 1) будут рассмотрены структурные альтернативы по регулированию этих сфер (раздел 2). В разделе 3 выявлены основные задачи, стоящие перед регулятором, связанные с проблемой определения персональных данных, их защиты и деперсонализации. В разделе 4 произведена оценка стимулов компаний по внедрению качественной киберзащиты в условиях новых регуляторных норм по обороту персональных данных.

## Специфичность больших и персональных данных

Исходя из формальных определений, большие данные[4] и персональные данные[5] являются пересекающимися множествами. По данным Росстата (НИУ ВШЭ, 2024) в 2022 г. в совокупности 27% организаций активно использовали источники больших данных, потенциально направленные на сбор информации, относящейся к персоналиям (веб-сайт, социальные сети, операторы сотовой сети). Однако стоит понимать, что не вся информация, которую оставляет человек (и которую собирает компания), строго может быть отнесена к «персональной», т.е. по которой можно прямо или косвенно можно идентифицировать субъекта. Но из-за отсутствия четких границ в определениях компании вынуждены перестраховываться — и хранить, и обрабатывать такие данные как персональные. Несмотря на то что рынок больших данных в России по некоторым оценкам растет (РБК, 2023), но до сих пор обмен и продажа баз данных и технологий затруднен как между бизнесами, так и с государством, что является в том числе следствием регуляторной неопределенности.

В основе возникновения различных точек зрения на регулирование больших данных лежит различное понимание специфичности этого ресурса. Согласно теории управления трансакциями О. Уильямсона (Уильямсон, 1996) под специфичностью активов понимается соотношение выгод и издержек от использования актива в рамках конкретной трансакции и выгод и издержек использования в альтернативных трансакциях. Понятие специфичности ресурса важно с точки зрения теории управления трансакциями: чем более специфичен ресурс, тем более специфичными становятся и отношения по поводу него, сложнее ввести государственное регулирование или разобраться третьей стороне в особенностях контрактации.

**Специфичность больших и персональных данных как ресурса.** С одной точки зрения, цифровые данные распространены повсеместно: они генерируются большим количеством персональных и иных устройств, подключенных к интернету. Цифровые данные влекут за собой практически нулевые предельные издержки сбора и передачи, а также неисключаемы и неконкурентны в потреблении. Более того, никакая отдельная фирма не в силах помешать кому-либо собирать и использовать большие данные, и такие базы могут эксплуатироваться многими фирмами

[4] Большие данные (big data) — большие массивы данных, отличающиеся главным образом такими характеристиками, как объем, разнообразие, скорость обработки и/или вариативность, которые требуют использования технологии масштабирования для эффективного хранения, обработки, управления и анализа (ГОСТ, 2021).

[5] Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон, 2006).

одновременно, не теряя при этом своей ценности (Competition Policy International, 2021). Поэтому фирмы могут воспринимать и сами большие данные, и их источники как неспецифические ресурсы (Lambrecht, Tucker, 2015). Согласно этой позиции, большие данные — это неконкурентный ресурс. То, что компании воспринимают информацию как неконкурентный и неспецифичный ресурс, может подтвердить позиция Ассоциации больших данных (далее — Ассоциация). В мерах, которые необходимы по мнению Ассоциации, для развития отрасли особо обозначаются возможность передачи анонимных персональных данных на коммерческой основе для широкого спектра целей (Ассоциация больших данных, 2023).

Однако стоит обратить внимание, что большие данные представляют собой не только некоторый набор информации, но они также требуют специфических средств обработки. Такое ПО может привнести определенную специфичность в отношения по поводу больших данных, так как оно предопределяет возможности компании по анализу данных и прогнозированию (Lambrecht, Tucker, 2015).

Персональные данные обладают высокой специфичностью для различных стороны рынка: пользователей, бизнеса и государства. Использование личной информации без согласия пользователя, скорее всего, не только несет в себе материальные риски (например, утекшие паспортные данные могут привести к поддельным кредитам), но и воспринимается как нарушение базовых прав. Регулятор, выступая гарантом базовых конституционных норм (как, например, ст. 23 Конституции РФ, дающее право на неприкосновенность частной жизни и личной переписки и иных сообщений), выступает на стороне потребителей. Множественные утечки персональных данных воспринимаются регулятором не только с точки зрения потери специфичной и существенной для пользователя информации, но и с точки зрения сохранности «национального ресурса».

**Специфичность цели использования больших данных.** Большие данные характеризуются тем, что их можно использовать для различных целей внутри компании при различных методах и способах обработки и анализа. В то же время, персональные данные, собираемые компаниями, могут быть направлены на достижение специфических целей — логистических (например, доставка товара), маркетинговых и рекламных задач (персонифицированная реклама, специальные предложения). Поэтому, персональные данные обладают специфичностью и для компаний, если их рассматривать с точки зрения целей использования. Персональные данные могут быть деперсонализированы, при этом, они потеряют часть своей специфичности (и поэтому, такие обезличенные данные могут быть переданы третьим лицам).

Для сбора персональной информации необходимо подтверждение пользователя на обработку точного набора данных конкретным опера-

тором на определенные цели. А. И. Савельев подчеркивает, что законодательные ограничения по обработке персональных данных вступают «в противоречие с существующей технологией и бизнес-практиками, поскольку оно нивелирует те преимущества, которые предоставляют технологии «больших данных» (Савельев, 2015).

Иными словами, можно наблюдать расхождение в понимании специфичности с точки зрения цели для разных типов данных — персональные данные являются более специфичным ресурсом (как минимум, если цель заранее оговаривается в соглашении), а большие данные в целом могут иметь множество неспецифицированных заранее целей использования.

## Структурные альтернативы регулирования сфер больших и персональных данных

На выбор механизма управления трансакциями влияет не только специфичность ресурса, но и уровень неопределённости[6]. Под уровнем неопределенности, как правило, понимается насколько агенты на рынке могут быть уверены в соблюдении достигнутых договоренностей, насколько контрагенты склонны к оппортунизму (может ли оппортунистическое поведение быть выгодно и сложно ли обойти действующие нормы). Уровень неопределенности зависит и от действующего законодательства — насколько оно склонно к изменениям, насколько силён инфорсмент, и каковы гарантии защиты соблюдения прав.

С точки зрения сферы больших данных на уровень неопределенности в правовой сфере оказывают воздействие текущие или планируемые изменения в законодательстве, «серые зоны» в законодательстве о больших данных, противоречивые решения судебной системы, внешние по отношению к сфере больших данных шоки — например, санкции.

Различный уровень специфичности больших и персональных данных приводят к различным структурным альтернативам по регулированию. Согласно теории механизмов координации О. Уильямсона, чем выше специфичность ресурса, тем более эффективной становится такая форма управления трансакциями, как иерархия. В данном случае становится понятно стремление усилить контроль за персональными данными.

В России отсутствует особое регулирование рынков больших данных, определяющими нормативными актами являются законы, касающиеся персональных данных (рис. 1а). Такой статус больших данных повышает

[6] Также имеет место критерий частоты трансакций, но он играет большую роль на уровне самих предприятий, когда они принимают решение о форме взаимодействия по поводу больших данных. С точки зрения альтернатив регулирования большее значение имеет аспект неопределенности.

уровень неопределённости, что приводит к комбинации механизмов координации: присутствует и контроль государства, и рыночный обмен, а также существуют саморегулируемые организации (например, Ассоциация).

Крайней альтернативой является «иерархия», что в рассматриваемой ситуации означает государственный контроль не только персональных данных, но и всей области больших данных (рис. 1б). Это может выражаться в различных механизмах — стандартизации механизмов обращения, лицензирование компаний и/или технологий (ПО), вплоть до создания государственного единого оператора больших данных. Главная проблема со всеми механизмами государственного контроля — технологическая. Бюрократический аппарат из-за негибкости, длительному нормотворческому процессу, медленной адаптации к технологическим изменениям не может «догнать» тенденции цифровых компаний, даже недавно принятые ГОСТы в сфере больших данных устарели на 6–7 лет и не учитывают последних новаций в IT-сфере (Ведомости, 2021). Однако для этой альтернативы имеются и преимущества — в виде стандартизации, что упрощает обмен между B2B (но даже прежде всего — B2G), а также чуть менее остро стоит вопрос об определении обезличенных (деперсонализированных) данных.

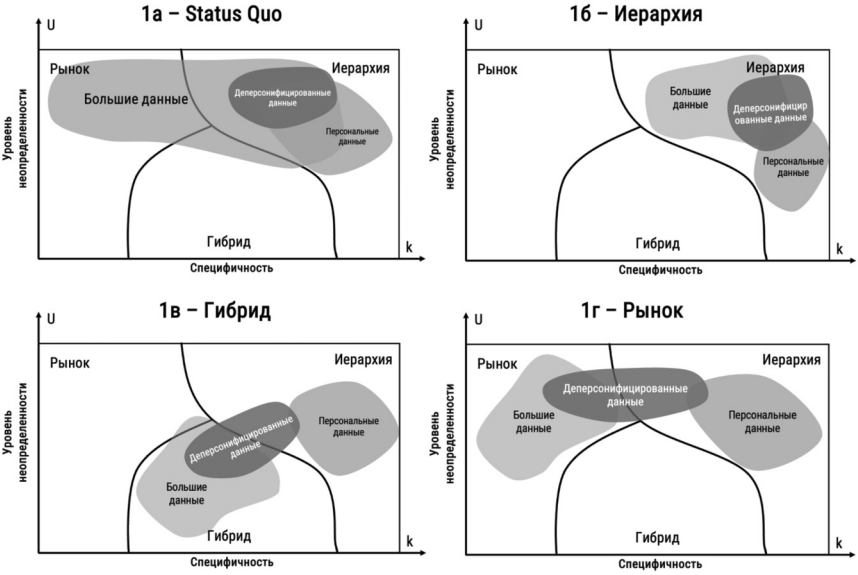


*Рис. 1.* Структурные альтернативы механизмов координации в сферах больших и персональных данных
*Источник*: составлено автором.

Рыночный подход (рис. 1г) к обороту больших данных свойственен США, где нет специализированного федерального регулирования, но применяется частичный секторальный подход. Такой подход дает возможность беспрепятственного обмена данными между компаниями, что стимулирует инновационную активность и дает толчок для развития малых и средних предприятий (МСП) в цифровой сфере (стартапов). Защита информации строится также на рыночных механизмах — так как компании в случае инцидентов (например, утечек) несут большие финансовые потери из-за необходимости ликвидации последствий, при этом велика роль репутационных потерь. Однако в нормативных документах США нет определений ни «персональных данных», ни «больших данных». В российских реалиях «повернуть вспять» и отменить определения не получится, можно лишь уточнять их, да и в целом подход к защите (и государственному доступу) к персональным данным отличается высоким уровнем контроля.

В нестабильных экономических условиях и при высокой скорости технологических изменений наибольшую ценность представляют собой гибридные механизмы (рис. 1в), позволяющие с большой скоростью адаптироваться и нормативную среду, к таким механизмам можно отнести саморегулируемые организации (СРО). Существующая в России с 2018 г. СРО (Ассоциация), прежде всего, выступает за создание бизнес-ориентированной стратегии в сфере больших данных, и представляет интересы только коммерческих фирм, что может нести в себе риски для потребителей, что можно сгладить привлечением аналитических центров и НИИ. В свою очередь, государственные регуляторы в связке с СРО должны не только гарантировать защиту персональных данных, но и установить «основные правила игры», ответив на два главных вопроса: (1) как «отделить» сферы больших данных и персональных данных друг от друга, (2) как определить статус обезличенных данных.

## Проблема определений персональных и обезличенных данных

Для устранения регуляторных противоречий необходимо «размежевание» сферы персональных данных и сферы больших данных, которое позволит снять напряжение между намерениями компаний по эффективному использованию больших данных и усилением контроля за безопасностью индивидуальных пользователей. Как было показано в первой части статьи, ключом к этому может послужить различная степень специфичности данных. Определение персональных данных должно идти через призму целей использования. К персональным данным должно относиться не только то, что позволяет однозначно определить человека, но и, по сути, связаться с ним (посредством телефона, электронной почты, адреса, статического

IP-адреса). Говоря простыми словами, персональные данные помогают компании: 1) идентифицировать уникального пользователя; 2) связываться с ним; 3) делать персональные акции и предложения. Также именно такая персональная информация не используется в качестве больших данных: номер паспорта, адрес электронной почты и телефон не играют роли в анализе потребительского поведения. Однако до сих пор у регулятора нет четкого понимания, что входит в «жесткое ядро» персональных данных — например, Верховный суд РФ (Определение Верховного Суда РФ, 2023) принял решение о том, что адрес электронной почты не является персональной информацией. Данное решение компаниями и юристами было оценено как неоднозначное (Denuo, 2023), и даже Минкомсвязь России рекомендовало всё же не снижать уровень защиты этого типа данных (Петров, 2021).

Компании заинтересованы в анализе выявленных потребительских предпочтений, которые чаще всего выражающихся в так называемых «цифровых следах». Но здесь справедливым будет вопрос — а можно ли по только по «цифровому следу» (исключая информацию, относящуюся к предполагаемому «жесткому ядру» персональных данных) определить субъекта персональных данных? Этот вопрос напрямую касается проблемы с определением обезличенных/деперсонализированных данных.

В 2024 г. в Государственной думе был принят Федеральный закон от 08.08.2024 № 233-ФЗ о деперсонализации данных, который дает возможность передавать обезличенные данные государству без дополнительного согласия пользователей, а также вводит возможность получения согласия пользователей сразу на несколько целей.

В Требованиях Роскомнадзора (Роскомнадзор, 2013) свойствами обезличенных данных являются: «обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность)» и «возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов)» (Роскомнадзор, 2013).

В приказе перечислены различные технические методы обезличивания: метод введения идентификаторов, метод изменения состава или семантики, метод декомпозиции, метод перемешивания. Там же имеется обязательное требование ко всем этим методам — об обратимости данных, т. е., по сути, обезличенные данные все равно подпадают под действие закона «О персональных данных». Это подтверждается как в научных юридических работах (Ohm, 2010), так и экспертами (Садовников, 2021).

Федеральный закон № 233 (от 08.08.2024) направлен на улучшение оборота больших данных между компаниями и государством, но не акцентирует внимание на основной преграде — обеспечении сохранности персональной информации. Главной проблемой остается возможность деобезличивания данных, которое возможно на основе следующей информации:

- использования данных из других открытых или имеющихся закрытых источников. Показательным примером является успешная попытка деанонимизации пользователей сервиса Netflix в 2006 г. Сервис выложил в открытый доступ статистику оценок фильмов и сериалов по каждому пользователю без личной информации. Но на основе других источников — IMDb и социальных сетей были восстановлены личности 84% пользователей (Майер-Шенбергер, Кукьер, 2017);
- использование данных из «утекших» баз данных. Данные, которые можно приобрести в «даркнете» зачастую содержат очень чувствительную и личную информацию, позволяющую достаточно легко объединить базы данных и деанонимизировать пользователя. Важно подчеркнуть, что для таких случаев особо полезными являются базы данных, постепенно утекающие из государственных сервисов и служб. Например, в сети можно найти базу ГИБДД, содержащую обширную информацию (более 50 млн записей) об автомобилях и их владельцах (Коммерсант, 2021) с 2006 г. по текущее время. Такие утечки информации, как правило, ускользают от внимания Роскомнадзора, так как данные «утекают» небольшими порциями и постепенно и отрицаются самими органами (ТАСС, 2019); использование информации, заключенной в самой базе данных — проблема критерия степени обезличенности данных. Некоторые возможные механизмы обезличивания данных являются достаточно простыми способами шифрования, например, замена ФИО на некий индекс, определяемый по какому-то установленному принципу. Современные технологии отличаются достаточной мощностью и возможностями по взлому механизмов шифрования, а быстрое развитие области искусственного интеллекта может поспособствовать тому, что подобные механизмы можно будет легко обойти и восстановить изначальные данные.

Из перечисленных выше аспектов следует, что проблема обезличенности данных шире, чем простая оценка того, содержит ли база данных «жесткое ядро» персональных данных (например, ФИО, номер паспорта, номер телефона). Без технологий, которыми обладают сами участники рынка, государственным органам невозможно справиться с обеспечением должной степени защиты информации, а также и с оценкой сте-

пени защиты и обезличивания данных. Поэтому построение рыночных отношений в области больших данных и налаживание контрактации невозможно без участников отрасли через взаимодействие с СРО. В текущем изложении нормативных документов требование по «обратимости» обезличенных данных не дает предпосылок для открытого обмена информацией.

С одной стороны, в областях, где высока скорость развития технологий, введение какого-либо регулирования и контроля может помешать эффективности. С другой стороны, область больших данных явно пересекается с областью персональных данных, которые являются значимым ресурсом, в том числе с точки зрения национальной безопасности. Поэтому стратегия регулирования этой области должна смещаться в сторону гибридного механизма, где могут быть учтены интересы как самих компаний, так и пользователей. Но для этого изначально должны быть уточнено определение «персональных данных», что снизит уровень неопределённости для всех задействованных сторон.

## 1. Оценка стимулов компаний по обеспечению кибербезопасности

Федеральный закон от 30.11.2024 № 420-ФЗ, ужесточающий штрафы по нарушению обращения персональных данных, возник в качестве необходимой меры для стимулирования компаний к выбору лучшего уровня защиты этих данных. Увеличение уровня штрафов и уровня инфорсмента должны подтолкнуть компании к использованию более совершенных средств защиты, однако они принимают решение об этом не только исходя из государственного регулирования, но из собственных издержек — как непосредственных затрат на обеспечение кибербезопасности, так и возможных репутационных потерь. В 2022 г. были приняты меры, влияющие на уровень инфорсмента в этой области — компании должны сами оповещать Роскомнадзор о возникшей утечке, а также в трехдневный срок проводить внутреннее расследование о причинах. До 2024 г. уровень штрафов являлся достаточно низким и не зависел от масштаба «утечки» и размера компании[7]. Новое регулирование вводит два вида штрафов — при первичном нарушении — фиксированная сумма, при вторичном (и последующих) нарушениях — «оборотные штрафы»[8]. Однако «оборотные» штрафы имеют верхнюю и, что главное, нижнюю границу, которая является единой для предприятий всех размеров.

[7] Для юридических лиц от 60 тыс. до 100 тыс. руб., за повторное нарушение — 500 тыс. рублей — ч. 1 ст. 13.11 КоАП.

[8] При первичном нарушении: если произошла утечка данных от 1000 до 10 000 субъектов персональных данных, штраф для юридических лиц — от 3 до 5 млн руб.; за утечку дан-

Внедрение Общего регламента по защите данных (General Data Protection Regulation, GDPR) показало, что ужесточение регулирования персональных данных негативно сказывается, прежде всего, на МСП, которые, тратят относительно большую долю средств на разработку и поддержание технической и программной инфраструктуры. Исследования демонстрируют, что это снижает уровень инноваций (Blind et al/, 2022; Jia et al., 2019) и инвестиций (Koski, Valmari, 2020; Chen et al., 2022) в цифровом секторе экономики, или же вовсе приводит к снижению конкуренции (Peukert et al., 2022; Geradin et al., 2021) в некоторых отраслях (прежде всего, в рекламном). В текущих условиях в России подобные эффекты могут быть еще сильнее, учитывая экономическую нестабильность и рост инфляции, а также кризис в сфере аппаратного обеспечения.

Для демонстрации эффективности вводимых мер рассмотрим упрощенную модель принятия решений компанией о внедрении системы киберзащиты, основанную на подходе Г. Беккера (Becker, 1986). Следует сделать оговорку, что решение о внедрении или улучшении систем кибербезопасности предприятиями является достаточно сложным процессом внутри компании, которая затрагивает не только сферы персональных и больших данных, поэтому представленные численные результаты следует воспринимать как примерную оценку достаточности и эффективности стимулов только в рассматриваемых областях.

Согласно модели, каждая компания принимает решение о необходимости усиления технической защиты в зависимости от внешних и внутренних условий: стоимости дополнительных технических вложений (C), вероятности «взлома» систем (q), а также вероятности (p) и объема наказания (F) со стороны регулятора, если утечка будет зафиксирована. Пусть фирма получает некоторый доход W, для достижения которого необходимо использование персональных данных. Фирма может вложиться в киберзащиту, затратив C, и при этом снизив вероятность успешности кибератак. Если компания не вкладывает в защиту — вероятность «взлома» $q_2$ выше, чем у фирмы, которая повысила уровень защиты ($q_2 > q_1$).

Любая компания не зависимо от того, какой уровень киберзащиты у нее есть, сталкивается с утечками данных, но вероятности такого события будут различаться. Утечки информации могут случаться и по вине собственных сотрудников, поэтому даже при высокой степени защиты вероятность утечки будет отлична от 0. В случае, если утечка произошла, компания терпит убытки в размере L.

---

ных — 10 000–100 000 субъектов — от 5 до 10 млн руб.; более 100 000 граждан — от 10 до 15 млн руб.

При повторном нарушении: при утечке персональных данных в объеме не менее 1000 записей — оборотный штраф от 0,1 до 3% выручки за календарный год, предшествующий нарушению, или за часть текущего года, но не менее 25 и не более 500 млн руб.

Получается, что компания, принимая решение о внедрении дополнительной технической защиты, руководствуется следующим алгоритмом (рис. 2).

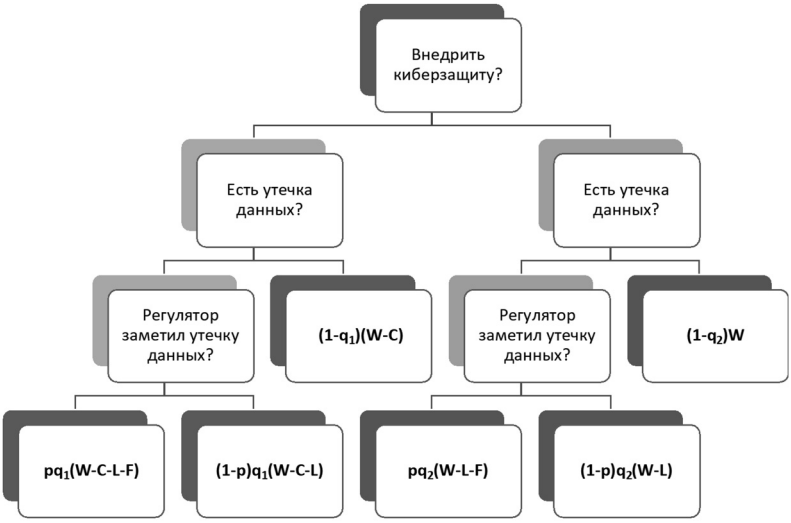


*Рис. 2.* Прибыль при различных решениях об уровне киберзащиты
*Источник:* составлено автором.

Компания будет вкладывать в техническую защиту, если ожидаемая прибыль от этого, будет выше, чем при условии, когда компания не несет дополнительные издержки (формула (1)):

$$W - C - pq_1F - q_1L > W - pq_2F - q_2L. \quad (1)$$

То есть компания будет инвестировать в киберзащиту, если будет выполняться следующее условие (формула (2)):

$$C < (q_2 - q_1)(L + pF). \quad (2)$$

Видно, что для компании, которая выбирает инвестировать или нет в усиление киберзащиты, важными являются не только потенциальные потери от взлома систем или от возможного штрафа (с поправкой на инфорсмент), но и надежность этих систем ($q_2 - q_1$) — насколько эта защита усилит устойчивость от взломов.

Оценку затрат на кибербезопасность (C) проводила компания «Лаборатория Касперского» по итогам 2022 г. (Лаборатория Касперского, 2023). Это исследование основано на интервью с 3230 респондентами, работающими в компаниях различного размера, от малого и среднего бизнеса

с числом сотрудников более 50 человек до крупных корпораций. По этим данным средние затраты на кибербезопасность в 2022 г/ у крупных компаний (с числом сотрудников более 1000 человек) составили $3750000, для МСП — 150 000 долл. В стоимость затрат на внедрение кибербезопасности входят стоимость программного обеспечения, так и оплата рабочей силы.

В моделировании была использована информация о возможных последствиях из-за утечек данных из трех источников, но все они основаны на опросах компаний. Полученные оценки сильно различаются из-за методологии и возможных смещений в оценке потерь самих опрашиваемых компаний (табл. 1).

*Таблица 1*

**Стоимость последствий утечки данных, долл.**

| | **МСП** | **Крупные компании** |
|---|---|---|
| Лаборатория Касперского по 2022 г. | 7694 | 104 488 |
| Лаборатория Касперского по 2020 г. | 118 000 | 1 343 000 |
| IBM по 2022 г. | 4 450 000 | |

*Источник:* Лаборатория Касперского, 2023; Лаборатория Касперского, 2021; IBM, 2023.

Расчеты будут производиться по всем трем источникам данных[9], так как, по сути, они отражают различие в оценке последствий утечек самих предприятий. Компания может подходить к вопросу оценки потерь достаточно точечно, воспринимая ущерб от конкретной утечки только как затраты на её ликвидацию (как в случае данных «Лаборатории Касперского за 2022 г.), а может включать в оценку «длинный хвост» различных потерь — от затрат на информирование до репутационных потерь (оценки IBM).

В модели будут рассмотрены различные оценки вероятности поимки утечки информации регулятором (p) — в интервале (0,4–1). По данным Роскомнадзора 80% операторов персональных данных вовремя уведомляют об утечках в 2023 г. (Интерфакс, 2023), что означает достаточно высокий уровень инфорсмента. Уровень штрафов взят из статей КОАП РФ: до вступления № 420-ФЗ в силу (30 мая 2025 г.) и после.

Для расчета эффективной величины штрафов введем следующие предпосылки, позволяющие получить минимальные оценки эффективных штрафов:

[9] Стоимость затрат на внедрение кибербезопасности и потери от утечек информации были конвертированы в рубли по курсу 70 руб. за доллар: как средний курс за 2020 г., и курс, действующий на начало 2023 г. (для данных Касперского и IBM).

– утечка данных при введении компанией киберзащиты невозможна ($q_1 = 1$);
– при отсутствии технической защиты утечки персональных данных неизбежны ($q_2 = 0$).

Полученные расчёты штрафов являются суммой, полученной вне зависимости от вида штрафа (фиксированный или оборотный), и отражают примерный порядок денежных выплат, которые стимулируют компанию на внедрение киберзащиты (табл. 2 и 3).

*Таблица 2*

**Минимальная величина эффективных штрафов (руб.) (данные «Лаборатории Касперского за 2022 г.)**

| Вероятность наказания (штрафа) | Крупные компании | МСП |
|---|---|---|
| 0,4 | 637 964 600,00 | 24 903 550,00 |
| 0,5 | 510 371 680,00 | 19 922 840,00 |
| 0,6 | 425 309 733,33 | 16 602 366,67 |
| 0,7 | 364 551 200,00 | 14 230 600,00 |
| 0,8 | 318 982 300,00 | 12 451 775,00 |
| 0,9 | 283 539 822,22 | 11 068 244,44 |
| 1 | 255 185 840,00 | 9 961 420,00 |

*Источник:* расчет авторов на основе данных Лаборатории Касперского, 2023.

*Таблица 3*

**Минимальная величина эффективных штрафов (руб.) (данные «Лаборатории Касперского за 2020 г.)**

| Вероятность наказания (штрафа) | Крупные компании | МСП |
|---|---|---|
| 0,4 | 464 391 666,67 | 8 108 333,33 |
| 0,5 | 371 513 333,33 | 6 486 666,67 |
| 0,6 | 309 594 444,44 | 5 405 555,56 |
| 0,7 | 265 366 666,67 | 4 633 333,33 |
| 0,8 | 232 195 833,33 | 4 054 166,67 |
| 0,9 | 206 396 296,30 | 3 603 703,70 |
| 1 | 185 756 666,67 | 3 243 333,33 |

*Источник:* расчет авторов на основе данных Лаборатории Касперского, 2021.

Вводимые штрафы при первой утечке для малых компаний уже сами по себе являются эффективными. Полученные расчеты (по обоим вариантам данных) совпадают с предлагаемой «вилкой» штрафов — от 3 млн до 15 млн руб. (в зависимости от объема данных). Получается, что новое регулирование окажется достаточно стимулирующим для принятия решения МСП о вложении инвестиций в кибербезопасность.

Если рассматривать полученные расчетные значения штрафов как оборотные штрафы для крупных компаний, зависящие от размера выручки, то они соответствуют предлагаемым мерам (не менее 25 и не более 500 млн руб.). В случае МСП — вводимые оборотные штрафы являются чрезмерными, так как они превышают размер эффективных в несколько раз.

Дополнительно в модели исследовалось эффективное качество кибербезопасности (которое отражается в выражении $(q_2\text{-}q_1)$. Результаты показали, что усиление инфорсмента и увеличение штрафов снижает ожидания компаний об ожидаемой степени защиты, то есть компании будут готовы внедрять киберзащиту, если она снижает вероятность «утечки» хотя бы на 45%. Однако для крупных цифровых компаний главным определяющим фактором все же являются собственные потенциальные потери от утечек, а не государственный инфорсмент. При этом очень важным фактором выступает то, как фирма рассматривает понятие «потерь от утечек» — включает ли только издержки, потраченные на ликвидацию инцидента, или же более широкий спектр затрат — вплоть до репутационных потерь. Однако существующий «парадокс конфиденциальности» (privacy paradox) (Marthews, Tucker, 2019; Моросанова, 2023) снижает значимость репутационных рисков.

Также для МСП играет роль объем персональной информации, которой они оперируют: если данные в компании становятся «большими», то такая компания более охотно внедрит киберзащиту, даже если она дает прирост в степени устойчивости от взлома в 20–40%.

Вводимые оборотные штрафы являются необходимой и назревшей мерой для российской цифровой сферы: учитывая стоимость внедрения системы кибербезопасности и возможные частные потери бизнеса от утечек. Увеличение штрафов уравновесит чашу весов между издержками на поддержание систем кибербезопасности и рисками, связанными с утечками информации. Однако стоит рассмотреть вопрос о введении механизма снижения уровня санкций для «честных» компаний, которые пытались предотвратить возможные внешние воздействия и инвестировали в высококачественную техническую защиту. Но остаются не решенными вопросы о качестве систем кибербезопасности: 1) достаточны ли стимулы для инвестирования в качественное ПО, 2) и главное — как оценивать качество этого ПО (а следовательно, уровень защиты). По сути, становится не ясным, как будет происходить процесс анализа того, до-

статочно ли компания сделала для предотвращения утечек информации или нет. В имеющейся судебной практике в России учитывалось то, приняла ли компания все необходимые по мнению суда меры для предотвращения утечки. Штрафы компаний за 2022–2023 гг. показывают, что как правило, он не назначается в максимальном размере (100 тыс. руб.), а остается на уровне чуть выше минимально возможного — 60 тыс. руб.: компании предоставляют доказательства, что защита от кибератак у компаний была внедрена, но технической внешней оценки надежности систем не проводилось.

Оценка качества надежности систем кибербезопасности является нетривиальной задачей, требующей «инсайдерской» информации и со стороны разработчиков, и со стороны пользователей этих систем. Даже в вопросах, связанных с расследованиями причин утечек информации, регулятору не справиться без дополнительного привлечения экспертов из отрасли. С 2022 г. стало сложнее классифицировать утечки информации по категориям «внешние» или «внутренние», большинство утечек имеют либо неопределенный, либо гибридный характер (57,5% от общего числа утечек) (InfoWatch, 2023). Любая техническая защита может не являться надежной с точки зрения взлома, если учитывать человеческий фактор. Снова, как и в вопросе деперсонализации, возникает необходимость сотрудничества государственных регуляторов и представителей бизнеса для разработки механизма оценки качества ПО, позволяющего адаптироваться как к технологическим изменениям на рынке, так и внешним шокам.

## Заключение

Для развития цифровой экономики требуется более свободный обмен большими данными, стимулирующий создание инноваций и более эффективную работу технологических компаний. Однако сфера больших данных тесно связана с областью персональной информации, так как частичный их объем генерируются за счет активных действий пользователей. Персональная информация является специфичным ресурсом и для самих пользователей, и для компаний, и для государства, в отличие от больших данных, которые могут использоваться для различных внутренних целей.

Различие в специфичности этих ресурсов может послужить основой для большего разделения этих двух сфер, что позволит с одной стороны, сохранить или даже усилить контроль за персональными данными, а с другой — заложить основы рынка больших данных, механизмов обмена или продажи больших данных между бизнесами и государством. Размытое определение персональных данных и противоречивые судебные решения не дают четких нормативных рамок, что значительно тормозит развитие сферы больших данных.

Одним из главных вопросов, который остро стоит перед регулятором — как гарантировать деперсонализацию (обезличивание) данных, таким образом, чтобы получившиеся базы не могли служить основой для их деанонимизации. В алгоритм оценки уровня обезличивания должны входить факторы, связанные с возможностями по агрегированию иных баз данных — как легальных (например, из открытых источников), так и «утекших» баз данных.

Из-за сильной связи персональных и больших данных Федеральный закон № 420-ФЗ по ужесточению контроля за оборотом персональной информации, может сказаться широко на всей цифровой сфере. Необходимо учитывать, что величина оборотных штрафов (а именно, условие штрафа — «не менее 25 млн руб.») может быть чрезмерной для МСП. Показательным примером среднесрочного негативного воздействия ужесточения регулирования на экономические показатели на цифровых рынках служит введение GDPR.

Технологические вопросы, связанные с деперсонализацией данных и с оценкой уровня качества киберзащиты, приводят к необходимости сотрудничества государства и бизнеса через саморегулируемые организации.

## Список литературы


Ассоциация больших данных. (2023). *Стратегия 2024.* Дата обращения 30.05.2024, https://rubda.ru/deyatelnost/strategiya/

Ведомости. (2021, 15 июля). *В России утвержден первый национальный стандарт в области больших данных.* Дата обращения 30.05.2024, https://www.vedomosti.ru/technology/articles/2021/07/15/878242-utverzhden-pervii-standart-v-oblasti-bolshih-dannih

ГОСТ Р 59925-2021. (2021). *Национальный стандарт Российской Федерации. Информационные технологии. Большие данные. Техническое задание.*

Интерфакс. (2023, 21 сентября). *РКН получает вовремя сигналы об утечках от 80% операторов персональных данных.* Дата обращения 30.05.2024, https://www.interfax.ru/russia/921948

Коммерсантъ. (2021, 22 октября). *База припарковалась у хакеров*. Дата обращения 30.05.2024, https://www.kommersant.ru/doc/5041801

Лаборатория Касперского. (2021). *Аналитический отчет «IT Security Economics 2020: Part 2»*. Дата обращения 30.05.2024, https://www.kaspersky.com/blog/it-security-economics-2020-part-2/

Лаборатория Касперского. (2023). *Аналитический отчет «2022 IT Security Economics Report»*. Дата обращения 30.05.2024, https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Economics%202022_report.pdf.

Майер-Шенбергер, В., & Кукьер, К. (2017). *Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим.* Манн, Иванов и Фербер.

Моросанова, А. А. (2023). Усиление регулирования защиты персональных данных в России: экономические последствия и риски. *Управленец, 14(5),* 29–46. https://doi.org/10.29141/2218-5003-2023-14-5-3.

НИУ ВШЭ. (2024). *Сборник «Индикаторы цифровой экономики 2024»*. Дата обращения 30.05.2024, https://issek.hse.ru/mirror/pubs/share/892389163.pdf

Определение Верховного Суда РФ от 21 июля 2023 г. N 305-ЭС23-12160 по делу N А40-139096/2022 (2023, 26 декабря).

Осипов, Ю. М. Юдина, Т. Н., & Купчишина, Е. В. (2020). «Искусственный интеллект», большие данные как институты экономики нового технологического поколения. *Вестник Московского университета. Серия 6: Экономика, 4,* 27-46. https://doi.org/10.38050/01300105202042

Петров, А. (2021, 14 ноября). *Являются ли e-mail и IP-адрес персональными данными?* Дата обращения 30.05.2024, https://pravo.rg.ru/rubrics/question/38477/

РБК. (2023, 04 декабря). *Как будет развиваться рынок больших данных в России*. Дата обращения 30.05.2024, https://trends.rbc.ru/trends/industry/cmrm/65688df29a7947662df7ba7a

Роскомнадзор. (2013). *Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных»*.

Савельев, А. И. (2015). Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data). *Право. Журнал Высшей школы экономики, 1*, 43–66.

Садовников, Д. (2021, 05 ноября). *Обезличивание персональных данных в России и в Европе: когда данные перестают быть персональными?* Zakon.ru. Дата обращения 30.05.2024, https://zakon.ru/blog/2021/11/5/obezlichivanie_personalnyh_dannyh_v_rossii_i_v_evrope_kogda_dannye_perestayut_byt_personalnymi

ТАСС. (2019, 21 ноября). *Утечки конфиденциальной информации: почему их все больше и как с ними бороться*. Дата обращения 30.05.2024, https://tass.ru/opinions/7164059

Уильямсон, О. (1996). *Экономические институты капитализма: Фирмы, рынки, «отношенческая» контрактация*. СПб.: Лениздат; CEV Press.

Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 30.11.2024 № 420-ФЗ. (2024, 30 ноября).

Федеральный закон «О внесении изменений в Федеральный закон “О персональных данных” и Федеральный закон “О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона “О персональных данных” от 08.08.2024 № 233-ФЗ. (2024, 8 «августа).

Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. (2006, 27 июля).

Шаститко, А. Е., Курдин, А. А., & Филиппова, И. Н. (2023). Мезоинституты для цифровых экосистем. *Вопросы экономики, 2,* 61–82. https://doi.org/10.32609/0042-8736-2023-2-61-82

Becker, G. (1986). Crime and Punishment: An Economic Approach. *Journal of Political Economy, 76* (2), 169–217. https://doi.org/10.1086/259394

Blind, K., Niebel, C., & Rammer, C. (2022). The impact of the EU General Data Protection Regulation on innovation in firms. *ZEW Discussion Papers, 22-047.* https://doi.org/10.2139/ssrn.4257740

Chen, C., Frey, C. B., & Presidente, G. (2022). Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *The Oxford Martin Working Paper Series on Technological and Economic Change. Working Paper No. 2022-1.*

Competition Policy International. (2021). *CPI Antitrust Chronicle February 2020.* Retrieved 30.05.2024, https://www.competitionpolicyinternational.com/wp-content/uploads/2020/02/CPI-Modrall.pdf

Denuo. (2023, 30 августа). *Верховный суд РФ не признал адрес электронной почты персональными данными.* Дата обращения 30.05.2024, https://denuo.legal/ru/insights/news/230830/

Geradin, D., Karanikioti, T., & Katsifis, D. (2021). GDPR Myopia: how a well-intended regulation ended up favouring large online platforms — the case of ad tech. *European Competition Journal, 17*(1), 47-92. https://doi.org/10.1080/17441056.2020.1848059

IBM Security. (2023). *Cost of a Data Breach Report.* Retrieved 30.05.2024, https://www.ibm.com/reports/data-breach

InfoWatch. (2023). *Утечки информации ограниченного доступа в мире, 2022 г.* Retrieved 30.05.2024, https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g

Jia, J., Zhe, J., & Wagman. L. (2019). The Short-Run Effects of GDPR on Technology Venture Investment. *NBER Working Papers 25248, National Bureau of Economic Research, Inc.* https://doi.org/10.2139/ssrn.3278912

Koski, H., & Valmari, N. (2020). Short-term Impacts of the GDPR on Firm Performance. *ETLA Working Papers. 77. The Research Institute of the Finnish Economy.*

Lambrecht, A., & Tucker, C. (2015). Can Big Data Protect a Firm from Competition. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.2705530

Marthews, A., & Tucker, C. (2019). Privacy policy and competition. *Brookings report. Brookings Economic Studies*, 1–27.

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review, 57,* 1701-1776.

Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2022). Regulatory Spillovers and Data Governance: Evidence from the GDPR. *Marketing Science, 41*(4), 318-340. https://doi.org/10.1287/mksc.2021.1339

## References

Association of Big Data. (2023). *Strategy 2024.* Retrieved 05/30/2024, https://rubda.ru/deyatelnost/strategiya/

Denuo. (2023, August 30). *The Supreme Court of the Russian Federation did not recognize email address as personal data.* Retrieved 05/30/2024, https://denuo.legal/ru/insights/news/230830/

Determination of the Supreme Court of the Russian Federation of July 21, 2023, No. 305-ES23-12160 in case No. A40-139096/2022 (2023, December 26).

Federal Law “On Personal Data” of July 27, 2006 No. 152-FZ. (2006, July 27).

Federal Law “On Amendments to the Code of Administrative Offenses of the Russian Federation” of November 30, 2024 No. 420-FZ. (2024, November 30).

Federal Law “On Amendments to the Federal Law ‘On Personal Data’ and the Federal Law ‘On Conducting an Experiment to Establish Special Regulation in Order to Create

the Necessary Conditions for the Development and Implementation of Artificial Intelligence Technologies in a Constituent Entity of the Russian Federation — the Federal City of Moscow and Amending Articles 6 and 10 of the Federal Law 'On Personal Data'" of August 8, 2024 No. 233-FZ. (2024, August 8).

GOST R 59925-2021 (2021). National standard of the Russian Federation. Information Technology. Big data. Technical task.

GOST R 59925-2021. (2021). *National standard of the Russian Federation. Information technology. Big data. Technical specification.*

InfoWatch. (2023). *Leaks of restricted access information in the world, 2022.* Retrieved 05/30/2024 https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g

Interfax. (2023, September 21). *RKN receives timely signals about leaks from 80% of personal data operators.* Retrieved 05/30/2024, https://www.interfax.ru/russia/921948

Kaspersky Lab. (2021). *Analytical report "IT Security Economics 2020: Part 2".* Retrieved 05/30/2024, https://www.kaspersky.com/blog/it-security-economics-2020-part-2/

Kaspersky Lab. (2023). *Analytical report "2022 IT Security Economics Report*". Retrieved 05/30/2024, https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Economics%202022_report.pdf.

Kommersant. (2021, October 22). *The database parked with hackers.* Retrieved 05/30/2024, https://www.kommersant.ru/doc/5041801

Mayer-Schoenberger, W., & Cukier, K. (2017). *Big data. A revolution that will change the way we live, work and think.* Mann, Ivanov and Ferber.

Morosanova, A. A. (2023). Strengthening personal data regulation in Russia: Economic implications and risks. *The Manager, 14 (5),* 29–46. https://doi.org/10.29141/2218-5003-2023-14-5-3

National Research University Higher School of Economics. (2024). *Collection "Digital Economy Indicators 2024".* Retrieved 05/30/2024, https://issek.hse.ru/mirror/pubs/share/892389163.pdf

Osipov, Yu. M. Yudina, T. N., & Kupchishina, E. V. (2020). "Artificial intelligence", big data as economic institutions of the new technological generation. *Moscow University Economic Bulletin. Series 6: Economics, 4*, 27-46. https://doi.org/10.38050/01300105202042

Petrov, A. (2021, November 14). *Are email and IP address personal data?* Retrieved 05/30/2024, https://pravo.rg.ru/rubrics/question/38477/

RBC. (2023, December 04). *How the big data market will develop in Russia.* Retrieved 05/30/2024, https://trends.rbc.ru/trends/industry/cmrm/65688df29a7947662df7ba7a

Roskomnadzor. (2013). *Methodological recommendations for the application of Roskonadzor order No. 996 dated September 05, 2013 "On approval of requirements and methods for anonymization of personal data."*

Sadovnikov, D. (2021, November 05) *Depersonalization of personal data in Russia and Europe: when does data cease to be personal?* Zakon.ru. Retrieved 05/30/2024, https://zakon.ru/blog/2021/11/5/obezlichivanie_personalnyh_dannyh_v_rossii_i_v_evrope_kogda_dannye_perestayut_byt_personalnymi

Savelyev, A. I. (2015). Problems of applying legislation on personal data in the era of Big Data. Right. *Journal of the Higher School of Economics, 1*, 43–66.

Shastitko, A. E., Kurdin, A. A., & Filippova, I. N. (2023). Meso-institutions for digital ecosystems. *Voprosy Ekonomiki, 2,* 61-82. https://doi.org/10.32609/0042-8736-2023-2-61-82

TASS. (2019, November 21). *Leaks of confidential information: why there are more and more of them and how to deal with them*. Retrieved 05/30/2024, https://tass.ru/opinions/7164059

Vedomosti. (2021, July 15). *The first national standard in the field of big data has been approved in Russia*. Retrieved 05/30/2024, https://www.vedomosti.ru/technology/articles/2021/07/15/878242-utverzhden-pervii-standart-v-oblasti-bolshih-dannih

Williamson, O. (1996). *Economic institutions of capitalism: Firms, markets, "relational" contracting*. St. Petersburg: Lenizdat; CEV Press.