Дата поступления рукописи в редакцию: 03.05.2026 г.
Дата принятия рукописи в печать: 14.05.2026 г.
DOI: 10.24412/2224-9133-2026-4-211-216

ЕРЕМИЧЕВ Ф.С.,
Аспирант Университета «Синергия»,
e-mail: fedor.eremichef@yandex.ru

КОЛЛЕКТИВНЫЕ ИСКИ КАК МЕХАНИЗМ ГРАЖДАНСКО-ПРАВОВОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ: ЗАРУБЕЖНЫЙ ОПЫТ И ПЕРСПЕКТИВЫ ИМПЛЕМЕНТАЦИИ В РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО

Аннотация. *В статье исследуется институт коллективных исков как механизм гражданско-правовой защиты персональных данных при массовых нарушениях. Проводится сравнительно-правовой анализ моделей коллективных исков в США, Европейском союзе и Китае. Выявляются основные проблемы действующего российского законодательства, препятствующие эффективной защите прав субъектов персональных данных при массовых утечках. Обосновывается необходимость введения специального механизма коллективных исков по делам о защите персональных данных. Предлагается авторская модель коллективного иска, учитывающая как зарубежный опыт, так и особенности российской правовой системы.*

Ключевые слова: *коллективный иск, персональные данные, утечка данных, массовые нарушения, гражданско-правовая защита, компенсация вреда, зарубежный опыт, имплементация.*

EREMICHEV F.S.,
Graduate student
of Synergy University

CLASS ACTIONS AS A MECHANISM OF CIVIL PROTECTION OF PERSONAL DATA: FOREIGN EXPERIENCE AND PROSPECTS FOR IMPLEMENTATION INTO RUSSIAN LEGISLATION

Annotation. *The article examines the institution of class actions as a mechanism of civil law protection of personal data in cases of mass violations. A comparative legal analysis of class action models in the USA, the European Union and China is conducted. The main problems of the current Russian legislation that hinder the effective protection of the rights of personal data subjects in cases of mass data breaches are identified. The necessity of introducing a special mechanism of class actions for personal data protection cases is substantiated. An original model of class action is proposed, taking into account both foreign experience and the specifics of the Russian legal system.*

Key words: *class action, personal data, data breach, mass violations, civil law protection, compensation, foreign experience, implementation.*

Массовые утечки персональных данных, затрагивающие сотни тысяч и миллионы граждан, стали одной из наиболее острых проблем цифровой эпохи. Действующее российское законодательство не содержит эффективного механизма коллективной защиты прав субъектов персональных данных при массовых нарушениях. Каждый пострадавший вынужден обращаться в суд индивидуально, что создает чрезмерную нагрузку на судебную систему и делает судебную защиту экономически нецелесообразной для большинства пострадавших с учетом низких размеров присуждаемых компенсаций [1].

Зарубежный опыт свидетельствует о высокой эффективности коллективных исков как инструмента защиты прав субъектов данных при массовых нарушениях. В США механизм коллективных исков (class action) обеспечил выплату компенсаций на сотни миллионов долларов пострадавшим от утечек персональных данных [2]. В Европейском союзе статья 80 GDPR пред-

усматривает право субъекта данных уполномочить некоммерческую организацию на подачу жалобы и осуществление прав от его имени [3]. Целью настоящей статьи является обоснование необходимости введения института коллективных исков в российское законодательство и разработка авторской модели данного института.

Анализ правоприменительной практики российских судов по делам о защите персональных данных выявляет ряд системных проблем, существенно снижающих эффективность индивидуальной судебной защиты при массовых нарушениях. Прежде всего, при массовых утечках персональных данных, затрагивающих значительное число субъектов, каждый пострадавший вынужден обращаться в суд самостоятельно, нести расходы на юридическую помощь, доказывать факт нарушения, причинно-следственную связь и размер причиненного вреда. При этом средний размер компенсации морального вреда по данной категории дел остается крайне низким [1].

Экономическая нецелесообразность индивидуального обращения в суд является ключевым фактором, объясняющим, почему подавляющее большинство нарушений остается без судебной реакции. Расходы на юридическую помощь по данной категории дел, как правило, существенно превышают размер ожидаемой компенсации. Даже с учетом возможности взыскания судебных расходов с ответчика экономическая мотивация для обращения в суд отсутствует. Это приводит к тому, что операторы не несут реальной гражданско-правовой ответственности за нарушения [4].

Информационная асимметрия между субъектом данных и оператором представляет собой еще одну существенную проблему. Оператор располагает полной информацией о порядке обработки персональных данных, применяемых мерах безопасности, обстоятельствах утечки, в то время как субъект данных, как правило, не имеет доступа к данной информации. Бремя доказывания факта нарушения, причинно-следственной связи и размера причиненного вреда возлагается на истца, что в условиях информационной асимметрии представляет значительную трудность [5].

Проблема нагрузки на судебную систему также заслуживает внимания. При массовой утечке персональных данных, затрагивающей значительное число субъектов, даже если небольшая часть пострадавших обратится в суд, это создаст существенную нагрузку на судебную систему, поскольку каждое дело рассматривается индивидуально, хотя обстоятельства нарушения являются одинаковыми для всех пострадавших. Коллективный иск позволяет объединить все требования в рамках одного процесса, что существенно экономит ресурсы судебной системы [6].

Действующее российское процессуальное законодательство предусматривает институт группового иска, закрепленный в главе 22.3 ГПК РФ, введенной Федеральным законом от 18 июля 2019 года N 191-ФЗ. Однако данный институт существенно отличается от классического коллективного иска и имеет ряд ограничений, делающих его малоэффективным для дел о массовых нарушениях персональных данных. Для подачи группового иска необходимо присоединение к иску не менее 20 лиц. Групповой иск основан на модели opt-in (присоединения), а не на модели opt-out (отказа), что существенно ограничивает численность группы [7].

Американская модель коллективного иска (class action) является наиболее развитой и эффективной в мире. Правило 23 Федеральных правил гражданского судопроизводства устанавливает четыре условия допустимости коллективного иска: многочисленность класса (numerosity), наличие общих вопросов права или факта (commonality), типичность требований представителя класса (typicality) и адекватность представительства (adequacy of representation) [2].

В сфере защиты персональных данных коллективные иски стали основным инструментом гражданско-правовой защиты в США. Компания Equifax согласилась выплатить значительную сумму по коллективному иску в связи с утечкой персональных данных граждан. Мировое соглашение предусматривало создание фонда для компенсации пострадавшим, выплату штатам и федеральному регулятору, а также обязательство инвестировать в информационную безопасность [2]. Компания Meta (Facebook), которая признана в РФ экстремистской организацией, согласилась выплатить значительную компенсацию по коллективному иску в связи со скандалом Cambridge Analytica, в рамках которого персональные данные пользователей были переданы третьей стороне без их согласия [8].

Важнейшей особенностью американской модели является механизм opt-out: все лица, соответствующие критериям класса, автоматически включаются в число участников, если не заявят об отказе. Это обеспечивает максимальный охват пострадавших и создает мощные экономические стимулы для операторов по обеспечению надлежащей защиты данных. Механизм финансирования коллективных исков посредством гонорара успеха (contingency fee) обеспечивает доступность данного инструмента для граждан, не имеющих средств на оплату юридических услуг [9].

Особого внимания заслуживает практика применения Закона штата Иллинойс о конфиденциальности биометрической информации (BIPA), который предусматривает право на частный иск с компенсацией за каждое нарушение при сборе биометрических данных без согласия. На основании BIPA были предъявлены многочисленные коллективные иски к технологическим компаниям за использование технологии распознавания лиц без получения письменного согласия пользователей [10].

В Европейском союзе механизм коллективной защиты основан на статье 80 GDPR, которая предусматривает право субъекта данных уполномочить некоммерческую организацию на подачу жалобы и осуществление прав от его имени. Директива (ЕС) 2020/1828 о представительных исках (Representative Actions Directive) обязывает государства-члены обеспечить возможность подачи представительных исков уполномоченными организациями от имени группы потребителей, включая иски о защите персональных данных [3]. Данная модель отличается от американской тем, что право на подачу иска предоставляется не индивидуальным представителям класса, а специализированным некоммерческим организациям, что снижает риск злоупотреблений.

В Китае статья 70 PIPL предусматривает право прокуратуры и определенных организаций на предъявление исков в общественных интересах (public interest litigation) в случае, если обработка персональной информации затрагивает права и интересы большого числа лиц. Данный механизм является китайским аналогом коллективного иска и позволяет обеспечить защиту прав пострадавших при массовых нарушениях [11].

Для сравнительного анализа моделей коллективной защиты персональных данных в различных юрисдикциях обратимся к *таблице 1.*

Таблица 1. Сравнительный анализ моделей коллективной защиты персональных данных

Параметр	США (Class Action)	ЕС (GDPR, ст. 80)	КНР (PIPL, ст. 70)	Россия (ГПК, гл. 22.3)
Модель	Opt-out	Представительный иск	Иск в общественных интересах	Opt-in (групповой)
Субъект подачи	Представитель класса	Некоммерческие организации	Прокуратура, организации	Группа лиц (не менее 20)
Финансирование	Гонорар успеха	За счет организации	Государственное	За счет истцов
Охват пострадавших	Максимальный	Средний	Средний	Минимальный
Эффективность	Высокая	Средняя	Средняя	Низкая

Как следует из таблицы 1, американская модель коллективного иска является наиболее эффективной с точки зрения охвата пострадавших и создания экономических стимулов для операторов. Российская модель группового иска существенно уступает зарубежным аналогам по всем ключевым параметрам, что обосновывает необходимость ее реформирования.

На основе проведенного сравнительно-правового анализа предлагается авторская модель коллективного иска по делам о массовых нарушениях права на защиту персональных данных, основанная на следующих принципах. Принцип opt-out: все субъекты данных, чьи персональные данные были нарушены в результате конкретного инцидента, автоматически включаются в число участников класса, если не заявят об отказе в установленный срок. Принцип представительства: коллективный иск может быть предъявлен общественной организацией, осуществляющей деятельность в сфере защиты прав потребителей или защиты персональных данных, Роскомнадзором, а также одним или несколькими субъектами данных, уполномоченными на представление интересов класса [6].

Принцип единого решения: решение суда по коллективному иску является обязательным для всех участников класса, не заявивших об отказе. Принцип справедливого распределения: присужденная компенсация распределяется между участниками класса пропорционально объему нарушенных прав. Принцип фонда невостребо-

ванных сумм: суммы компенсации, не востребованные участниками класса в течение установленного срока, направляются в специальный фонд защиты персональных данных [12].

Механизм уведомления участников класса является ключевым элементом предлагаемой модели. Суд, принявший решение о рассмотрении дела в порядке коллективного иска, обязывает ответчика-оператора направить индивидуальное уведомление всем субъектам данных, чьи персональные данные были нарушены, с использованием имеющихся контактных данных. Одновременно уведомление публикуется на официальном сайте суда, на сайте Роскомнадзора и в средствах массовой информации. Расходы на уведомление возлагаются на ответчика-оператора [7].

Предлагается двухуровневая система распределения компенсации. На первом уровне все участники класса, не заявившие об отказе, получают базовую компенсацию в размере минимальной установленной законом суммы. На втором уровне участники класса, доказавшие конкретные убытки или особые нравственные страдания, получают дополнительную компенсацию, размер которой определяется судом индивидуально. Данная двухуровневая система обеспечивает, с одной стороны, гарантированную минимальную компенсацию для всех пострадавших, а с другой — справедливую дифференциацию для лиц, понесших наибольший вред [12].

Вопрос о финансировании коллективных исков имеет принципиальное значение для обеспечения доступности данного механизма. Для российского законодательства предлагается комбинированная модель: коллективные иски могут финансироваться как адвокатами на условиях гонорара успеха (с ограничением размера гонорара определенным процентом от присужденной суммы), так и общественными организациями, а также из средств специального фонда защиты персональных данных, формируемого за счет части оборотных штрафов [13].

Для наглядного представления предлагаемой модели коллективного иска обратимся к *рисунку 1.*



Рисунок 1. Схема предлагаемой модели коллективного иск

Как показано на рисунке 1, предлагаемая модель коллективного иска включает шесть последовательных этапов: от момента массового нарушения до распределения компенсации между пострадавшими и направления невостребованных сумм в специальный фонд. Данная

модель обеспечивает комплексную защиту прав субъектов персональных данных при массовых нарушениях и учитывает как американский опыт (модель opt-out, гонорар успеха), так и европейский (право общественных организаций на предъявление иска).

Для оценки потенциального эффекта от введения института коллективных исков обратимся к *таблице 2*, в которой представлено сравнение текущей ситуации и прогнозируемых результатов.

Таблица 2. Прогнозируемый эффект от введения коллективных исков

Показатель	Текущая ситуация	Прогноз после введения
Доля пострадавших, получающих компенсацию	Менее 0,1%	До 30–50%
Средний срок получения компенсации	4,5 месяца (судебное)	2–3 месяца
Совокупный размер компенсаций по одному инциденту	Незначительный	Существенный
Нагрузка на судебную систему	Множество индивидуальных исков	Один коллективный иск
Превентивный эффект для операторов	Минимальный	Существенный

Как следует из таблицы 2, введение института коллективных исков позволит существенно увеличить долю пострадавших, получающих компенсацию, сократить сроки ее получения и создать мощные экономические стимулы для операторов по обеспечению надлежащей защиты персональных данных.

Проведенное исследование позволяет сформулировать следующие основные выводы. Действующий механизм индивидуальной судебной защиты является неэффективным при массовых нарушениях права на защиту персональных данных. Институт группового иска, предусмотренный главой 22.3 ГПК РФ, не обеспечивает адекватной защиты при массовых утечках в силу модели opt-in, требования о минимальном числе участников и отсутствия специального механизма финансирования [7].

Зарубежный опыт свидетельствует о высокой эффективности коллективных исков как инструмента защиты прав субъектов данных при массовых нарушениях. Предлагаемая авторская модель коллективного иска, основанная на принципе opt-out, праве общественных организаций на предъявление иска и двухуровневой системе распределения компенсации, позволит обеспечить реальную защиту прав пострадавших граждан и создать эффективные экономические стимулы для операторов [12].

Реализация предлагаемой модели требует внесения изменений в Гражданский процессуальный кодекс Российской Федерации, Федеральный закон «О персональных данных» и ряд иных нормативных правовых актов. Представляется целесообразным поэтапное введение данного института с предварительной апробацией в рамках пилотного проекта [13].

Список литературы:

[1] Трофимова И.А., Питько Е.В. Особенности гражданско-правовой ответственности за нарушение норм, регулирующих защиту персональных данных работников // Пробелы в российском законодательстве. 2016. №3.

[2] In re Equifax Inc. Customer Data Security Breach Litigation, No. 1:17-md-2800 (N.D. Ga. 2019). Settlement Agreement.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Art. 80.

[4] Санникова Л.В. Гражданско-правовая защита персональных данных // Журнал российского права. 2023. N 8. С. 56–70.

[5] Исаев А.С., Хлюпина Е.А. Правовые основы организации защиты персональных данных. СПб: НИУ ИТМО, 2014. 106 с.

[6] Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 N 138-ФЗ (ред. от 31.07.2025).

[7] Федеральный закон от 18.07.2019 N 191-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

[8] In re Facebook, Inc. Consumer Privacy User Profile Litigation, No. 3:18-md-02843 (N.D. Cal. 2022). Settlement Agreement.

[9] Писарев В.В. Эволюция законодательства США об обороте персональных данных после принятия калифорнийского закона о конфиденциальности персональных данных потребителей // Образование и право. 2024. №6.

[10] Biometric Information Privacy Act (BIPA), 740 ILCS 14 (2008).

[11] Personal Information Protection Law of the People's Republic of China (PIPL), adopted 20.08.2021. Art. 70.

[12] Богатырева А.Т., Перепадя О.А., Чуниха А.А. Современные тенденции развития института персональных данных в условиях цифровизации // Право и государство: теория и практика. 2024. №9 (237).

[13] Федеральный закон от 30.11.2024 N 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

References:

[1] Trofimova I.A., Pitko E.V. Features of civil liability for violation of the norms governing the protection of personal data of employees//Gaps in Russian legislation. 2016. №3.

[2] In re Equifax Inc. Customer Data Security Breach Litigation, No. 1:17-md-2800 (N.D. Ga. 2019). Settlement Agreement.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Art. 80.

[4] Sannikova L.V. Civil protection of personal data//Journal of Russian Law. 2023. N 8. S. 56-70.

[5] Isaev A.S., Khlyupina E.A. Legal basis for the organization of personal data protection. St. Petersburg: NRU ITMO, 2014. 106 s.

[6] Civil Procedure Code of the Russian Federation of 14.11.2002 N 138-FZ (ed. 31.07.2025).

[7] Federal Law of 18.07.2019 No. 191-FZ "On Amendments to Certain Legislative Acts of the Russian Federation."

[8] In re Facebook, Inc. Consumer Privacy User Profile Litigation, No. 3:18-md-02843 (N.D. Cal. 2022). Settlement Agreement.

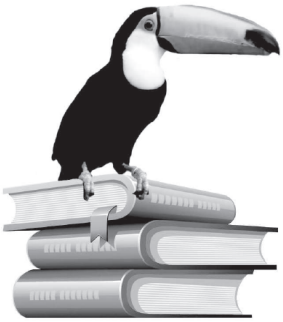
[9] V.V. Pisarev. Evolution of US legislation on the circulation of personal data after the adoption of the California law on the confidentiality of personal data of consumers//Education and law. 2024. №6.

[10] Biometric Information Privacy Act (BIPA), 740 ILCS 14 (2008).

[11] Personal Information Protection Law of the People's Republic of China (PIPL), adopted 20.08.2021. Art. 70.

[12] Bogatyreva A.T., Perapadya O.A., Chunikha A.A. Current trends in the development of the institution of personal data in the context of digitalization// Law and the state: theory and practice. 2024. №9 (237).

[13] Federal Law of 30.11.2024 No. 420-FZ "On Amendments to the Code of Administrative Offenses of the Russian Federation."



Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников, учебных и методических пособий, монографий, научных статей.

Профессионально.

В максимально короткие сроки.

Размещаем в РИНЦ, E-Library.

www.law-books.ru