

П. О. Лозовский¹✉, А. В. Шабурова¹

Роль организаций как операторов персональных данных

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: lozovskiy.log@mail.ru

Аннотация. Ежегодно в России правовое регулирование защиты персональных данных претерпевает изменения. Вносимые корректировки направлены на совершенствование нормативной базы и обеспечение соответствия высоким международным стандартам. Такая динамика позволяет эффективнее обеспечивать права и свободы граждан, прежде всего – право на неприкосновенность частной жизни. Особое значение в реализации этих гарантий приобретают организации – операторы персональных данных. Именно на них возлагаются обязанности по сбору, хранению, обработке и защите информации. В связи с растущими требованиями к конфиденциальности возникает необходимость детального анализа таких организаций, их функций и ответственности. Настоящая работа посвящена исследованию роли организаций как операторов персональных данных и выявлению проблемных аспектов их деятельности в контексте законодательства Российской Федерации.

Ключевые слова: Персональные данные, информация, защита, интернет, организация

P. O. Lozovsky¹✉, A. V. Shaburova¹

The Role of Organizations as Personal Data Controllers

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: lozovskiy.log@mail.ru

Abstract. Every year, the legal regulation of personal data protection in Russia undergoes changes. The adjustments being introduced are aimed at improving the regulatory framework and ensuring compliance with high international standards. Such dynamics make it possible to more effectively ensure the rights and freedoms of citizens, above all – the right to privacy. Of particular importance in the implementation of these guarantees are organizations acting as personal data controllers. They are entrusted with the obligations to collect, store, process, and protect information. Due to the growing requirements for confidentiality, there is a need for a detailed analysis of such organizations, their functions, and their responsibility. This paper focuses on examining the role of organizations as personal data controllers and identifying problematic aspects of their activities in the context of the legislation of the Russian Federation.

Keywords: Personal data, information, protection, internet, organization

Введение

В процессе оформления трудовых отношений по запросу работодателя сотрудник передает значительный объем документации и заполняет анкеты, содержащие разделы, которые относятся не только к профессиональной деятельности, но и затрагивают аспекты частной жизни: сведения о состоянии здоровья, наличие или отсутствие судимости, биометрические данные. При этом работник мо-

жет возражать против того, чтобы эти сведения становились известными широкому кругу лиц.

В связи с увеличением числа случаев хищения персонифицированной информации личные данные физического лица нуждаются в защите от несанкционированного доступа третьих лиц. В связи с этим проблема обработки и хранения персональных данных работника попадает в сферу особого внимания любой организации. При заключении трудовых отношений с работником организация приобретает статус оператора персональных данных и, принимая на себя обязанности по их защите, становится поднадзорной контролирующим органам [1].

В целях защиты конфиденциальной информации в Российской Федерации действует специальный правовой режим. Для его обеспечения в 2006 году был принят Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Кроме того, в статье 3 указанного Федерального закона закрепляется понятие «конфиденциальность персональных данных». «Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания» [4].

Цель данной научной статьи рассмотреть роль организаций как оператора персональных данных.

Методы и материалы

Развитие компьютерных технологий и глобальной сети Интернет привело к значительному увеличению количества информационных систем и баз данных, которые сегодня охватывают практически все сферы общественной жизни. Параллельно с этим компьютеры и Интернет обеспечили переход к более эффективным и быстрым процедурам сбора, хранения и структурирования персональной информации.

Существуют базы данных социального обеспечения, медицинской информации, правоохранительных органов, государственных, муниципальных информационных систем, компаний выпускающих кредитные карты и мобильные операторы. Организации являются активными потребителями этих данных и имеют решающее значение для успеха многих операций. Они фиксируют привычки, предпочтения и другие модели индивидуальной деятельности, которые помогают им разрабатывать, продвигать и продавать продукты и услуги.

В этой статье мы проанализируем роль организаций защиты персональных данных, при которой конфиденциальность по-прежнему защищена. Описание и анализ обезличивания персональных данных показывают надежную систему, которая может обеспечить такой уровень защиты конфиденциальности, который не мешает правительствам и организациям проводить статистические исследования. Эти данные важны и собираются для статистических целей.

Методами данного исследования является анализ литературы, синтез и обработка результатов анализа.

Результаты

В настоящее время организации в Российской Федерации приходится иметь дело с законами и нормативными актами о защите данных [1-5]. Такая фрагментация представляет собой дорогостоящее административное бремя, которое затрудняет доступ многих организаций, особенно малых и средних, к новым рынкам.

Согласно законодательству Российской Федерации, одной из основных обязанностей всех организаций, включая малые и средние предприятия, выступающие в качестве контролеров или обработчиков данных, является обеспечение безопасности персональных данных [4].

В частности, согласно внутреннему регламенту организаций, безопасность в равной степени охватывает конфиденциальность, целостность и доступность и должна рассматриваться с учетом рисков: чем выше риск, тем более строгие меры должен принимать контролер (для управления риском). Хотя такой подход к оценке рисков не является новой концепцией, было внедрено лишь несколько специальных систем оценки рисков для конфиденциальности, которые в основном сосредоточены на оценке рисков, связанных с персональными данными, и принятии соответствующих мер безопасности [10].

В то время как крупные организации имеют возможность реагировать на эти системы и внедрять их надлежащим образом, малые и средние предприятия не всегда обладают необходимыми знаниями и ресурсами для этого.

На самом деле, во многих случаях малым и средним предприятиям трудно понять конкретные риски, связанные с обработкой персональных данных, а также оценить эти риски и управлять ими, используя формальную методологию. Это может нанести ущерб малым и средним предприятиям, и в то же время затруднить выполнение ими юридических обязательств в соответствии с внутренним регламентом организаций.

На сегодняшний день существуют правовые, организационные, технические и программные методы защиты персональных данных сотрудников в организации [7].

Организационные меры – основа системы защиты персональных данных. К ним относятся:

Назначение ответственного за обработку персональных данных. Эту роль может выполнять кадровый сотрудник, юрист или привлеченная сторонняя организация. На указанное лицо возлагаются следующие функции: контроль за соблюдением правовых требований, разъяснение работникам правил обработки данных, а также рассмотрение обращений граждан по вопросам, связанным с их персональными данными. [11].

Данная мера предполагает четкое определение круга лиц, которым доступ к персональным данным необходим для выполнения должностных обязанностей. Утверждается перечень таких сотрудников, и с каждого из них берется подписка о неразглашении. В зависимости от типа данных и специфики организации к

числу уполномоченных лиц могут относиться руководители подразделений, специалисты определенных отделов или иные сотрудники [15].

Для каждой категории лиц или роли определяется минимальный набор прав, необходимый для выполнения рабочих задач. Например, в ролевой модели управления доступом права предоставляются на основе бизнес-функций, а не личности или стажа сотрудников [6].

Реализация технических мер осуществляется посредством применения средств защиты информации.

В рамках обеспечения информационной безопасности необходимо использование сертифицированных средств защиты. К числу таких средств относятся антивирусы, межсетевые экраны и системы обнаружения вторжений, каждое из которых обязано иметь актуальный сертификат ФСТЭК России либо ФСБ России [19].

Сертификация средств защиты информации проводится государственными и аккредитованными органами, а испытания – специализированными аккредитованными лабораториями, в отдельных случаях – на базе разработчика. Порядок аккредитации регулируется установленными нормативами. Органы сертификации и испытательные центры несут ответственность за корректность процедур, сохранность конфиденциальной информации и соблюдение прав заявителя.

Системы управления доступом (IAM) обеспечивают безопасное управление идентификацией, аутентификацией и авторизацией пользователей в ИТ-среде. Они предусматривают строгую (в том числе двухфакторную) аутентификацию, позволяют точно идентифицировать действия пользователей и предоставляют доступ к данным только уполномоченным лицам по принципу минимально необходимых прав [20].

IAM разграничивает права доступа: сотрудникам предоставляются только необходимые функции (например, просмотр или редактирование), что снижает риск ошибок и обеспечивает стабильную работу. Также в IAM входят компоненты, работающие вместе для обеспечения безопасности и организации процесса:

Защита каналов передачи данных и шифрование. Вся передача персональных данных по открытым каналам связи (в том числе при удаленной работе) должна шифроваться. [12]

Уведомление Роскомнадзора. До начала обработки персональных данных организация обязана уведомить Роскомнадзор о намерении их обрабатывать. Форма уведомления утверждена Приказом Роскомнадзора от 28.10.2022 № 180 [5].

Получение согласия субъекта на обработку данных. Согласие требуется, если это не вытекает из закона или договора. В обязательном порядке согласие нужно для распространения данных, в том числе для публикации на сайте [8].

Заключение договоров с подрядчиками. Если данные передаются на аутсорсинг (например, в облако), договор должен обязывать подрядчика защищать информацию так же, как это делает организация.

Обсуждение

Мы остановимся на управлении идентификацией и доступом (IAM) в облаке как основной мере защиты персональных данных сотрудников.

Выявим основные проблемы данного метода защиты.

Ниже перечислены основные проблемы, с которыми сталкиваются организации при управлении идентификацией и доступом (IAM) в облаке:

1. Управление большим количеством пользователей и устройств.

В облачных средах множество пользователей, устройств и приложений, которым необходим доступ. Отслеживание того, кто и что может делать для каждого пользователя и устройства, может очень быстро стать сложной задачей, особенно по мере роста организации [16].

2. Работа с несколькими облачными провайдерами (мультиоблачная среда).

Многие организации используют более одного облачного сервиса (например, Mail облако, Yandex диск, Google Cloud). Управление доступом на всех этих различных платформах с помощью собственных инструментов IAM может быть сложным и запутанным, а обеспечение согласованности – непростой задачей.

3. Обеспечение надлежащего уровня доступа.

Предоставление пользователям слишком большого доступа рискованно, но предоставление слишком малого доступа может заблокировать работу. Найти правильный баланс (так называемый «минимальный уровень привилегий») и обеспечить обновление доступа по мере изменения ролей – большая проблема.

4. Защита от угроз безопасности.

Облачные системы постоянно подвергаются кибератакам. Система управления идентификацией и доступом (IAM) должна быть достаточно надежной, чтобы предотвратить несанкционированный доступ пользователей, но хакеры постоянно находят новые способы это сделать. Кража учетных данных, фишинг или внутренние угрозы затрудняют эту задачу [14].

Фишинг представляет собой метод социальной инженерии, при котором злоумышленники посредством поддельных электронных сообщений, имитирующих письма банков и иных организаций, побуждают пользователей раскрывать персональные и конфиденциальные данные. Данный вид атак становится все более опасным из-за усложнения методов обмана пользователей [9].

5. Управление жизненным циклом идентификации.

Существенная динамика увольнений и найма в организации накладывает ответственную роль на системы управления. Системы управления идентификацией и доступом (IAM) должны быстро обновляться или удалять доступ, чтобы избежать сохранения старых или некорректных разрешений, создающих риски безопасности [17].

6. Соблюдение нормативных требований и аудит.

Во многих отраслях действуют строгие правила относительно того, кто имеет доступ к каким данным. Системы управления идентификацией и доступом (IAM) должны надлежащим образом отслеживать и регистрировать все доступы, чтобы организации могли доказать соблюдение этих правил во время аудитов.

7. Сложность интеграции.

Система управления идентификацией и доступом (IAM) должна бесперебойно взаимодействовать со множеством различных облачных сервисов, приложений и локальных систем.

Заключение

В целях защиты персональных данных и соблюдения права на неприкосновенность частной жизни организации обязаны создать и обеспечить необходимую техническую и административную инфраструктуру.

Кроме того, им необходимо реализовать все необходимые правовые нормы в отношении действий, которые следует предпринять при получении персональных данных третьими лицами.

Внутренняя сеть организации объединяет все компоненты информационных систем организации и часто предоставляет точки подключения к внешним сетям. Она является как точкой входа, так и средством распространения атак. Поэтому защита внутренней сети имеет решающее значение [12].

Защита персональных данных должна быть интегрирована в цикл ИТ-разработки, начиная с этапа проектирования и для конфигураций по умолчанию, чтобы предоставить субъектам данных лучший контроль над своими данными и ограничить ошибки, потери, несанкционированные изменения или неправильное использование их данных в приложениях.

Любое действие, совершенное по неосторожности и содержащее ошибку, способно повлечь за собой, что неуполномоченные лица получают доступ к персональным данным, нарушая тем самым право субъектов данных на неприкосновенность частной жизни. Кроме того, организации, имеющие доступ к серверам, через которые передается информация, могут иметь доступ к их содержимому или метаданным.

Обработка данных, выполняемая обработчиком от имени контролера, должна быть обеспечена достаточными мерами предосторожности, в частности, с точки зрения безопасности. Оператор данных должен быть осведомлен о деталях мер безопасности, применяемых его обработчиками [18].

Чтобы иметь возможность идентифицировать мошеннический доступ или неправомерное использование персональных данных, а также определить причину инцидента, необходимо регистрировать определенные события, выполняемые в ИТ-системах.

Без принятия дополнительных мер каналы передачи данных (электронная почта, системы обмена мгновенными сообщениями, платформы хранения файлов) не являются безопасными средствами связи для передачи персональных данных [13].

Государство уделяет особое внимание обеспечению защиты персональных данных. Законодательное регулирование охватывает процессы сбора, хранения и обработки данных, включая персональные сведения граждан. Важным направлением является создание систем, обеспечивающих надежную защиту персональных данных, а также формирование сервисов, гарантирующих безопасность

информации граждан в цифровом взаимодействии. Таким образом, персональные данные выступают одновременно объектом регулирования, ресурсом для развития и приоритетом в сфере информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации от 12 декабря 1993 г. (в ред. от 05.10.2022 28.02.2025) [Электронный ресурс]. URL: <http://government.ru/docs/all/98196/> (дата обращения: 05.05.2026).
2. Гражданский Кодекс Российской Федерации от 26.11.2001 №146-ФЗ (в ред. от 08.08.2024) // Гарант [Электронный ресурс]. URL: <http://www.kremlin.ru/acts/bank/17547> (дата обращения: 05.05.2026).
3. Трудовой Кодекс Российской Федерации от 30 декабря 2001 №197-ФЗ (в ред. от 01.03.2026) // Гарант [Электронный ресурс]. URL: <https://docs.cntd.ru/document/901807664> (дата обращения: 05.05.2026).
4. Федеральный Закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 28.02.2025) // Гарант [Электронный ресурс]. URL: <http://www.kremlin.ru/acts/bank/24154> (дата обращения: 05.05.2026).
5. Приказ Роскомнадзора от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных» (ред. от 28.10.2022) // Гарант [Электронный ресурс]. URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=438326> (дата обращения: 05.05.2026).
6. Аверченков, В. И. Защита персональных данных в организации / В.И. Аверченков. - М.: Флинта, 2022. - 682 с.
7. Благодаров, Андрей Витальевич Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / Благодаров Андрей Витальевич. - М.: Горячая линия - Телеком, 2020. - 134 с.
8. Бойкова, Ольга Феоктистовна Защита персональных данных: касается всех! Практическое пособие. Выпуск № 142 / Бойкова Ольга Феоктистовна. - М.: Либерея, 2018. - 434 с.
9. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. - Москва: Огни, 2021. - 536 с.
10. Информационная безопасность открытых систем. В 2 томах. Том 2. Средства защиты в сетях / С.В. Запечников и др. - Москва: Высшая школа, 2019. - 560 с.
11. Информационная безопасность систем организационного управления. Теоретические основы. В 2 томах. Том 1. - М.: Наука, 2018. - 496 с.
12. Кин, Эндрю Ничего личного. Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные для собственной выгоды / Эндрю Кин. - М.: Альпина Пабlishер, 2021. - 224 с.
13. Мещеряков, Роман Валерьевич Защита персональных данных в организациях здравоохранения: моногр. / Мещеряков Роман Валерьевич. - М.: Горячая линия - Телеком, 2021. - 950 с.
14. Новая парадигма защиты и управления персональными данными в РФ и зарубежных странах в условиях развития систем обработки данных в сети Интернет / Коллектив авторов. - Москва: СИНТЕГ, 2019. - 296 с.
15. Новая парадигма защиты и управления персональными данными. - Москва: Наука, 2022. - 651 с.

16. Право доступа [Электронный ресурс]. URL: https://rt-solar.ru/products/solar_inrights/blog/4636/ (дата обращения: 10.05.2026).
17. Управление идентификацией и доступом. Руководство по IAM для начинающих [Электронный ресурс]. URL: <https://selectel.ru/blog/what-is-iam/> (дата обращения: 10.05.2026).
18. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2023. - 304 с.
19. Федоров, А. В. Информационная безопасность в мировом политическом процессе / А.В. Федоров. - М.: МГИМО-Университет, 2018. - 220 с.
20. Филиппов, П. Б. Использование и защита персональных данных в социальных сетях Интернета / П.Б. Филиппов. - М.: Синергия, 2023. - 106 с.

© П. О. Лозовский, А. В. Шабурова, 2026