

Обязательства сервиса и оферта

При сбоях многое зависит от того, что сервис обещал пользователям.

Что проверить заранее

Поэтому сначала стоит посмотреть оферту, тарифы и описание на сайте: какие функции должны быть доступны, что сказано о технических работах и что предусмотрено на случай длительного простоя. Эти условия лучше согласовать заранее. Изменение оферты после сбоя само по себе уже возникшие требования не снимет.

Ограничения ответственности

Формулировка о том, что сервис не несет ответственности за любые перебои, тоже не решает вопрос полностью. В договорах с бизнесом можно согласовать допустимые ограничения ответственности.

Права потребителя

Если пользователь — потребитель, лишить его установленных законом прав такой оговоркой нельзя. Например, безусловный запрет на возврат денег может оказаться ничтожным.

Ответственность хостинг-провайдера

Сбой у хостинга не освобождает сервис от ответственности автоматически. Нарушение обязательств провайдером само по себе не считается форс-мажором. Поэтому договор с провайдером стоит проверить заранее: что он гарантирует, как реагирует на инциденты и какую компенсацию можно потребовать.

Судебная практика и действия при сбое

ДЕЛО А56-85885/2024

1,28 млн ₽

реальный ущерб

около 4 млн ₽

упущенная выгода

Обстоятельства и вывод суда

Например, Арбитражный суд Северо-Западного округа отказал клиенту хостинг-провайдера во взыскании 1,28 млн рублей реального ущерба и около 4 млн рублей упущенной выгоды, возникших из-за временной недоступности сайта после DDoS-атаки. Ключевой вывод: защита от DDoS – это дополнительная услуга, и без ее заказа ответственность на провайдера не возлагается (дело А56-85885/2024).

Коммуникация с пользователями

Когда сбой уже произошел, пользователям лучше сообщить, какие функции недоступны, что команда делает и когда появится следующая информация. Обещать восстановление «через час», если техническая команда этого не подтверждает, не стоит. Переписку, логи и сведения о ходе восстановления нужно сохранить – они помогут разобраться с претензиями и подтвердить обстоятельства сбоя.

Если пользователи не уведомлены

Если сервис не уведомил пользователей о сбое, это само по себе может являться нарушением договорных обязательств и дает основания для требования компенсации. Можно заранее предусмотреть меры по компенсации отсутствия доступа к платформе/информации. Например, по аналогии с операторами связи, которые могут компенсировать абонентам время простоя двумя способами: уменьшить следующий платеж по тарифу или зачислить деньги на лицевой счет пропорционально времени недоступности услуги.

Персональные данные и инциденты

Проверка документов и инфраструктуры

По персональным данным придется проверить и документы, и фактическую работу сервиса: какие данные собираются, на каком основании, где хранятся, кому доступны и какие меры защиты приняты. При срочном переезде на другую инфраструктуру требования к локализации и трансграничной передаче продолжают действовать.

С 1 июля 2025 года

Локализация • ч. 5 ст. 18 Закона № 152-ФЗ

При этом важно учитывать актуальные требования: с 1 июля 2025 года изменена редакция требования о локализации персональных данных (ч. 5 ст. 18 Закона № 152-ФЗ). Теперь при сборе персональных данных граждан РФ через интернет запись, систематизация, накопление, хранение, уточнение и извлечение должны осуществляться с использованием баз данных, находящихся на территории России. Использование зарубежных облачных платформ для этих целей сопряжено с рисками нарушений. Поэтому лучше заранее подготовить всю информацию о том, как, где и в каком порядке хранятся персональные данные и принять превентивные меры по физической защите данных мест.

Когда нужно уведомить Роскомнадзор

Если выявлена утечка или неправомерный доступ к персональным данным, повлекшие нарушение прав людей, действуют сроки уведомления Роскомнадзора: 24 часа — на первичное сообщение, 72 часа — на результаты внутреннего расследования. Оба срока считаются с момента выявления инцидента.

Уведомления, штрафы и подготовка

24 часа

первичное сообщение

72 часа

результаты расследования

1–3 млн ₽

за сроки уведомления

до 20 млн ₽

за первичную утечку

Ответственность • ст. 13.11 КоАП РФ

За нарушение сроков уведомления предусмотрен штраф от 1 млн до 3 млн рублей, а максимальный размер штрафа за утечку персональных данных достиг 20 млн рублей при первичном нарушении в зависимости от объема и категории персональных данных (ст. 13.11 КоАП РФ).

Назначить ответственного заранее

Кто занимается уведомлением, лучше решить заранее: во время аварии на распределение обязанностей может просто не хватить времени.

Чек-лист защиты и договоров

1. Резервное копирование

- ☐ Создайте три копии, на двух разных типах носителей, одну расположите в другом регионе;
- ☐ Автоматизируйте бэкапы и раз в квартал проверяйте восстановление.

2. Защита данных

- ☐ Шифруйте базы и резервные копии;
- ☐ Персональные данные храните только на серверах в РФ (152-ФЗ);
- ☐ Разработайте качественную политику по обработке персональных данных в организации (соглашения, согласия, собственно политику и т.д.) и реализуйте ее постоянно;
- ☐ Минимальные права, надежные пароли, многофакторная аутентификация, регулярный пересмотр и отзыв лишних прав.

3. Договоры и форс-мажор

- ☐ В договорах с контрагентами пропишите форс-мажор, включая атаки;
- ☐ Проверьте соглашение с хостингом, гарантии доступности и компенсации;
- ☐ И помните, что сам факт атаки не освобождает от ответственности, нужно доказать невозможность исполнения.

Организационные меры

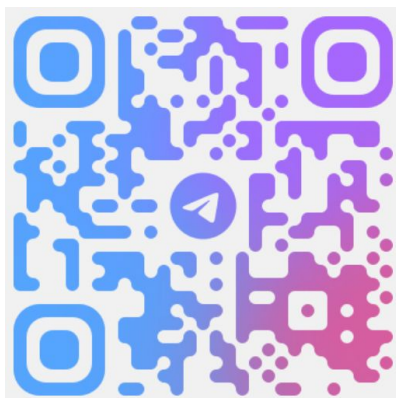
- ☐ Проведите учебную тревогу по сценарию утечки;
- ☐ Заранее назначьте ответственного за уведомления.

Действия при инциденте

Краткий план реагирования

- Уведомите Роскомнадзор за 24 ч (первично) и 72 ч (расследование);
- Сохраняйте логи, переписку и все доказательства.

Материал подготовлен компанией LAMP LEGAL



Telegram-канал LAMP LEGAL
[@lamp_room_legal](https://t.me/lamp_room_legal)



По вопросам аудита,
консультаций и сопровождения
[@lamp_request](https://t.me/lamp_request)