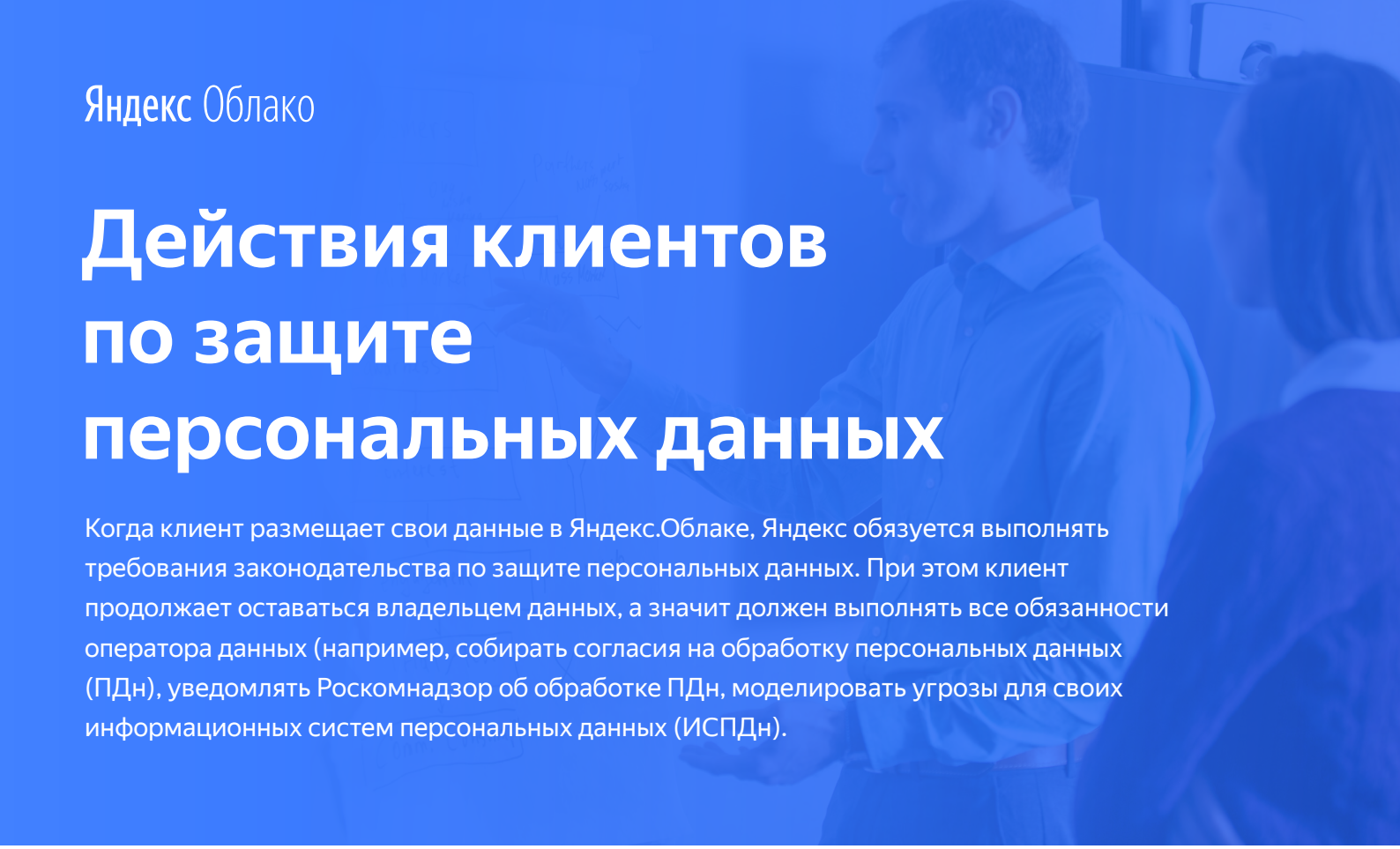
Яндекс Облако

Действия клиентов по защите персональных данных



Когда клиент размещает свои данные в Яндекс.Облаке, Яндекс обязуется выполнять требования законодательства по защите персональных данных. При этом клиент продолжает оставаться владельцем данных, а значит должен выполнять все обязанности оператора данных (например, собирать согласия на обработку персональных данных (ПДн), уведомлять Роскомнадзор об обработке ПДн, моделировать угрозы для своих информационных систем персональных данных (ИСПДн).

Действия оператора данных в области защиты ПДн можно условно разделить на:
— Формирование описательных и регламентных документов, требуемых законодательством.
— Реализация технических мер безопасности для систем, работающих поверх облачной инфраструктуры.

Клиент может реализовать эти требования самостоятельно или привлечь партнера Яндекс.Облака по информационной безопасности:
— компанию «Б-152»;
— компанию «Кард Секьюрити».

Если клиент обратился за помощью к партнёру Облака, эксперты партнёрской организации предоставят ему подробные инструкции. Если клиент решил самостоятельно реализовать требования, то он может ориентироваться на данный список действий:

1. Оценить бизнес-процессы, в рамках которых обрабатываются персональные данные. Определить цели обработки, состав обрабатываемых ПДн, порядок обработки ПДн, а также места и форму хранения ПДн. Определить законные основания обработки ПДн.

2. Оценить возможный ущерб субъектам ПД, провести моделирования угроз безопасности ПДн в ИСПДн.

3. Определить уровни защищенности ИСПДн согласно требованиям постановления правительства №1119.

4. Назначить работника, ответственного за организацию обработки персональных данных.

5. Сформировать меры по реализации требований Приказа №21 ФСТЭК России. Например, для реализации 3-го уровня защищённости могут быть применены следующие меры защиты:
   — Настройка средств аутентификации внутри виртуальных машин (на уровне ОС, СУБД, прикладного ПО).
   — Контроль доступа пользователей к виртуальным машинам (на уровне ОС, СУБД, прикладного ПО).
   — Регистрация событий безопасности (на уровне ОС, СУБД, прикладного ПО).
   — Реализация антивирусной защиты виртуальных машин.
   — Анализ уязвимостей и установка обновлений безопасности на ОС, СУБД и прикладное ПО.
   — Обеспечение защиты данных от раскрытия и модификации при передаче их через Интернет.
   — Управление изменениями внутри виртуальных машин.

6. Документировать и реализовать выбранные меры защиты и осуществлять периодический контроль их исполнения.

7. Разработать пакет локальных документов (политика, положения, регламенты и инструкции), регулирующие обработку и защиту персональных данных в организации.

8. Опубликовать политику в отношении обработки персональных данных на сайтах и в мобильных приложениях организации.

9. Подписать согласия на обработку персональных данных (в случае необходимости) с работниками и другими физическими лицами, чьи персональные данные вы обрабатываете.

10. При необходимости подать уведомление в Роскомнадзор об обработке ПДн.

11. Поддерживать документацию по персональным данным в актуальном состоянии.