ПРИКАЗ БЮРО ЗАЩИТЫ ДАННЫХ НЕО-СИТИ

№ 667

"О требованиях к использованию облачных сервисов для хранения и обработки персональных данных"

г. Нео-Сити
05 ноября 2089 года

В целях обеспечения надлежащей защиты персональных данных при их трансграничной передаче и обработке в облачных средах, в соответствии с требованиями статей 30-33 Кодекса о защите данных (трансграничная передача данных), Бюро защиты данных

ПРИКАЗЫВАЕТ:

1. Общие положения

1.1. Настоящий Приказ устанавливает требования к использованию облачных сервисов для хранения и обработки персональных данных операторами данных Нео-Сити.

1.2. Для целей настоящего Приказа:

а) *облачный сервис* — модель предоставления вычислительных ресурсов, хранилищ данных или программного обеспечения через сеть по требованию;

б) *облачный провайдер* — организация, предоставляющая облачные сервисы;

в) *IaaS (Infrastructure as a Service)* — предоставление инфраструктуры (серверы, хранилища);

г) *PaaS (Platform as a Service)* — предоставление платформы для разработки;

д) *SaaS (Software as a Service)* — предоставление программного обеспечения;

е) *регион размещения* — географическое расположение центров обработки данных провайдера.

1.3. Действие настоящего Приказа распространяется на:

а) операторов данных, использующих облачные сервисы для обработки персональных данных;

б) облачных провайдеров, предоставляющих услуги операторам Нео-Сити;

в) посредников и реселлеров облачных услуг.

2. Классификация облачных сервисов по уровню риска

2.1. Высокий риск — облачные сервисы для:

а) хранения специальных категорий данных (статья 4.2 КЗД);

б) обработки данных более 100,000 субъектов;

в) критической инфраструктуры;

г) финансовых и медицинских данных.

2.2. Средний риск:

а) хранение и обработка общих персональных данных;

б) данные 10,000-100,000 субъектов;

в) данные о транзакциях (статья 4.3 КЗД);

г) поведенческие данные (статья 4.4 КЗД).

2.3. Низкий риск:

а) данные менее 10,000 субъектов;

б) контактные данные;

в) публичные данные;

г) обезличенные данные.

2.4. Классификация определяет требования к выбору провайдера и защитным мерам.

3. Требования к выбору облачного провайдера

3.1. При выборе облачного провайдера оператор обязан провести оценку (due diligence), включающую:

а) анализ политики безопасности провайдера;

б) проверку сертификаций и аудитов;

в) оценку территориального размещения данных;

г) анализ SLA и гарантий;

д) проверку финансовой устойчивости;

е) оценку репутации и истории инцидентов.

3.2. Обязательные сертификации провайдера:

а) для высокого риска — ISO 27001, SOC 2 Type II, и сертификация Бюро защиты данных;

б) для среднего риска — ISO 27001 или SOC 2;

в) для низкого риска — документированная система управления безопасностью.

3.3. Территориальные требования:

а) для высокого риска — размещение данных только на территории Нео-Сити;

б) для среднего риска — территория Нео-Сити или страны с адекватным уровнем защиты (статья 31 КЗД);

в) для низкого риска — допускается размещение в иных странах при наличии надлежащих гарантий (статья 32 КЗД).

3.4. Перечень стран с адекватным уровнем защиты публикуется Бюро защиты данных.

4. Договорные требования

4.1. Договор с облачным провайдером должен содержать:

4.1.1. Обязательные положения:

а) предмет обработки (категории данных, операции);

б) роли сторон (оператор — обработчик);

в) инструкции по обработке данных;

г) обязательства по безопасности;

д) условия привлечения субподрядчиков;

е) обязательства по уведомлению об инцидентах;

ж) условия аудита;

з) условия возврата и удаления данных;

и) ответственность сторон.

4.1.2. Положения о безопасности:

а) конкретные меры защиты;

б) шифрование (при хранении и передаче);

в) контроль доступа;

г) мониторинг и журналирование;

д) управление уязвимостями;

е) план обеспечения непрерывности.

4.1.3. Положения о соответствии:

а) обязанность соблюдать КЗД и иные нормативные акты;

б) содействие в реализации прав субъектов данных;

в) уведомление об изменениях в законодательстве страны провайдера.

4.2. Для трансграничной передачи (статьи 30-33 КЗД) договор должен включать стандартные договорные условия, утверждённые Бюро защиты данных.

4.3. Оператор сохраняет копию договора в течение всего срока обработки и 5 лет после.

5. Технические требования к облачным сервисам

5.1. Шифрование:

а) данные шифруются при передаче (TLS 1.3);

б) данные шифруются при хранении (AES-256);

в) для высокого риска — шифрование ключами оператора (BYOK);

г) управление ключами документируется.

5.2. Контроль доступа:

а) многофакторная аутентификация;

б) ролевая модель доступа;

в) принцип минимальных привилегий;

г) регулярный пересмотр прав доступа;

д) журналирование всех операций доступа.

5.3. Изоляция данных:

а) логическое разделение данных разных клиентов;

б) для высокого риска — физическая изоляция (выделенная инфраструктура);

в) защита от несанкционированного доступа персонала провайдера.

5.4. Резервное копирование:

а) соответствие требованиям Приказа № 623;

б) размещение резервных копий в согласованных регионах;

в) возможность независимого резервного копирования оператором.

5.5. Портируемость данных:

а) возможность выгрузки данных в стандартных форматах;

б) API для миграции данных;

в) документированные процедуры миграции.

6. Права и обязанности оператора

6.1. Оператор остаётся ответственным за обработку персональных данных независимо от использования облачных сервисов.

6.2. Обязанности оператора:

а) выбор надлежащего провайдера;

б) заключение договора с необходимыми условиями;

в) документирование инструкций по обработке;

г) контроль за соблюдением инструкций;

д) реагирование на инциденты;

е) реализация прав субъектов данных;

ж) уведомление субъектов о месте обработки данных.

6.3. Права оператора:

а) проведение аудитов провайдера (самостоятельно или через аудитора);

б) получение отчётов о безопасности;

в) получение информации об инцидентах;

г) изменение или прекращение обработки;

д) получение данных при прекращении договора.

6.4. Оператор информирует субъектов данных об использовании облачных сервисов в политике конфиденциальности.

7. Обязанности облачного провайдера

7.1. Провайдер обязан:

а) обрабатывать данные только по инструкциям оператора;

б) обеспечивать конфиденциальность (обязательства персонала);

в) реализовывать согласованные меры безопасности;

г) привлекать субподрядчиков только с согласия оператора;

д) содействовать в реализации прав субъектов;

е) уведомлять об инцидентах;

ж) удалять данные по окончании обработки;

з) предоставлять информацию для аудитов.

7.2. Уведомление об инцидентах:

а) провайдер уведомляет оператора незамедлительно (в течение 24 часов);

б) уведомление содержит описание инцидента, затронутые данные, принятые меры;

в) провайдер содействует в расследовании.

7.3. Субподрядчики:

а) привлечение только с предварительного согласия оператора;

б) на субподрядчика распространяются те же обязательства;

в) провайдер несёт ответственность за действия субподрядчиков;

г) оператор информируется о перечне субподрядчиков.

8. Аудит и контроль

8.1. Оператор вправе проводить аудит провайдера:

а) самостоятельно или через независимого аудитора;

б) по согласованному графику или при наличии оснований;

в) с доступом к документации, системам, помещениям.

8.2. Провайдер предоставляет:

а) отчёты независимых аудитов (SOC 2, ISO 27001);

б) результаты тестов на проникновение;

в) журналы доступа к данным оператора;

г) информацию об инцидентах и уязвимостях.

8.3. Оператор проводит периодическую оценку провайдера:

а) для высокого риска — ежегодно;

б) для среднего риска — раз в 2 года;

в) для низкого риска — раз в 3 года.

8.4. При выявлении несоответствий оператор:

а) требует устранения в разумный срок;

б) усиливает контроль;

в) при неустранении — прекращает использование сервиса.

9. Прекращение использования облачного сервиса

9.1. При прекращении договора провайдер обязан:

а) вернуть данные оператору в согласованном формате;

б) удалить все данные из своих систем;

в) удалить данные у субподрядчиков;

г) предоставить подтверждение удаления.

9.2. Сроки:

а) возврат данных — в течение 30 дней;

б) удаление данных — в течение 60 дней после возврата;

в) подтверждение удаления — в течение 90 дней.

9.3. Оператор планирует стратегию выхода (exit strategy):

а) процедуры миграции данных;

б) альтернативные провайдеры;

в) временные решения на период миграции.

10. Ответственность

10.1. За использование провайдера без надлежащей оценки:

а) штраф 500,000-2,000,000 кредитов.

10.2. За отсутствие договора с необходимыми условиями:

а) штраф 1,000,000 кредитов.

10.3. За размещение данных в запрещённых регионах:

а) штраф до 4% годового оборота;

б) обязанность перенести данные.

10.4. За ненадлежащий контроль за провайдером:

а) штраф 500,000 кредитов;

б) обязанность провести аудит.

10.5. Оператор несёт ответственность перед субъектами данных за действия провайдера.

11. Переходные положения

11.1. Настоящий Приказ вступает в силу с 01 января 2090 года.

11.2. Операторы обязаны провести оценку существующих провайдеров до 01 апреля 2090 года.

11.3. Договоры с провайдерами должны быть приведены в соответствие до 01 июля 2090 года.

11.4. Бюро публикует перечень стран с адекватным уровнем защиты до 15 декабря 2089 года.

11.5. Бюро публикует стандартные договорные условия до 15 декабря 2089 года.

Директор Бюро защиты данных

Е.А. Морозова

Регистрационный номер: НС-БЗД-667/11-05

Опубликован: 10 ноября 2089 года