BCP и DRP глазами privacy

Резервирование, репликация, локализация ПД

Секция 1 | Данные и технологии

Лиана Ованканян | Юрист | Comply

Privacy is respect

1 Теория: цели privacy engineering по NIST

Триада ИБ

защищает данные

- **Конфиденциальность**
- **Целостность**
- **Доступность**

\+

Цели privacy engineering

NISTIR 8062 · защищают людей

Предсказуемость	понятно, что происходит с данными при сбое
Управляемость	данные можно найти и удалить, в т. ч. в копиях
Несвязываемость	шифрование и псевдонимизация копий

» Ст. 19 152-ФЗ: защищать ПД и от уничтожения, и от блокирования. Плохо спроектированное резервирование нарушает обе модели сразу

2 BCP и DRP: процесс, а не железо

BCP · Business Continuity Plan

Как бизнес продолжает работать при сбое: процессы, люди, приоритеты

DRP · Disaster Recovery Plan

Как восстанавливаем системы и данные: порядок, ответственные, сроки

Две метрики – и что они значат для ПД

RPO – сколько данных потеряем

RTO – сколько длится простой

10 р.д.
срок ответа субъекту



Последняя копия — **Сбой** — **Восстановление**

Для ПД: окно потерь
→ **целостность**

Для ПД: права субъекта не исполнить
→ **доступность**

2.1 Подходы к резервированию и ПД

Подход	Как работает	RPO / RTO	Что важно для ПД
Полный бэкап	Копия всех данных по расписанию	часы–сутки / часы	Сроки хранения и удаление копий
Инкрементальный бэкап	Только изменения с прошлой копии	часы / дольше (по цепочке)	Все звенья цепочки содержат ПД
Репликация	Синхронно или асинхронно – на резервный узел	≈0–минуты / минуты	Реплика – полноценная БД с ПД

» Резервные копии – на отдельной площадке, а не там же, где основная система и реплика

RPO и RTO – типичные порядки величин; фактические значения зависят от настроек

3 Резервирование и локализация

Сценарий	Можно?	Почему	Что оформить
Все узлы и копии в РФ	**Да**	Ч. 5 ст. 18 соблюдена	Все места БД – в уведомлении РКН
Бэкап или асинхронная реплика за рубежом	**Да, с условиями**	Сначала запись в РФ, затем трансграничная передача копии	Ст. 12: оценка, уведомление РКН, уничтожение
Синхронная реплика за рубежом	**Риск**	Запись подтверждается в РФ и за рубежом одновременно	Обосновать схему или держать синхронный узел в РФ
Переключение на резерв за рубежом	**Нет**	Резерв становится основной БД – новые записи идут за рубеж	Площадка для переключения – только в РФ

«Да, с условиями» – при первичной записи в РФ; это позиция регулятора на практике, а не прямая норма закона

4 8 стратегий privacy by design

Стратегия	Для резервирования
Minimize	Резервируем только нужное для восстановления
Hide	Шифруем копии, ключи храним отдельно
Separate	Разносим копии географически и логически
Aggregate	Для аналитики – агрегаты, а не сырые ПД

Стратегия	Для резервирования
Inform	Политика говорит, где и сколько хранятся копии
Control	Права субъекта работают и для копий
Enforce	Сроки хранения и ротация – автоматически
Demonstrate	Журналы, контроль целостности, тесты восстановления

Я.-Х. Хупман, Privacy Design Strategies – применительно к резервированию

5 Три вывода, которые стоит унести

- **Доступность и целостность – тоже требования 152-ФЗ**
- **Каждая копия и реплика – это персональные данные**
- **Первичная запись – только в РФ, даже при переключении на резерв**

Проверьте, где ваши копии и куда DR-план переключит запись



Лиана Оваканян

Юрист

Comply

comply.ru
t.me/comply_ru