МКБ

Защита данных. Жизнь без DLP

Жизненный цикл данных

Жизненный цикл данных

Ввод данных

Жизненный цикл данных

Ввод данных

Передача

Жизненный цикл данных

Ввод данных

Передача

Использование

Жизненный цикл данных

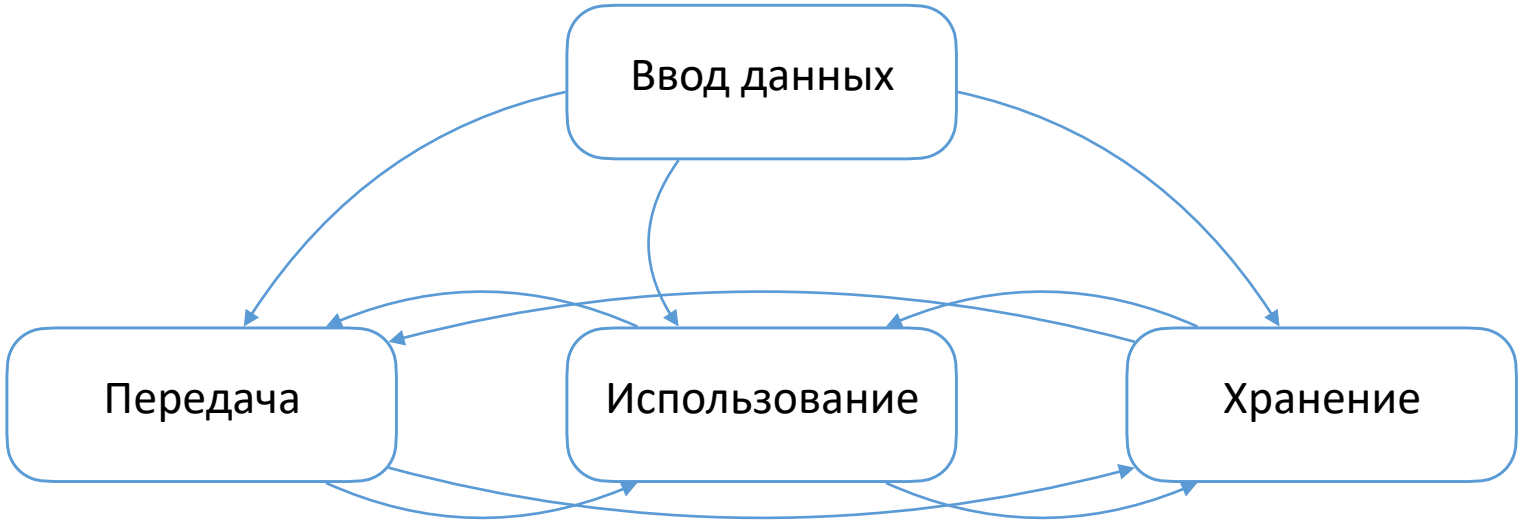
Ввод данных

Передача

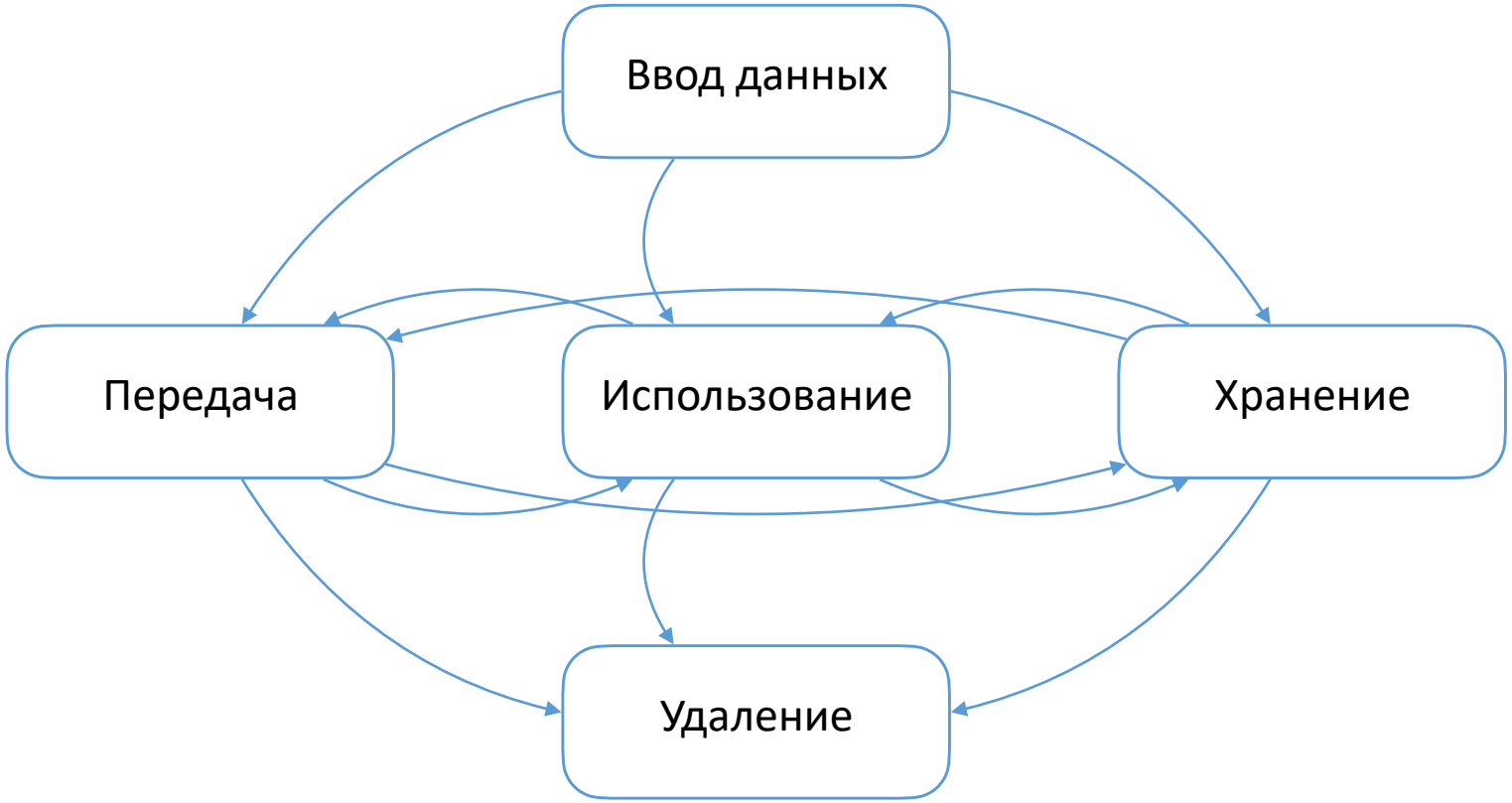
Использование

Хранение

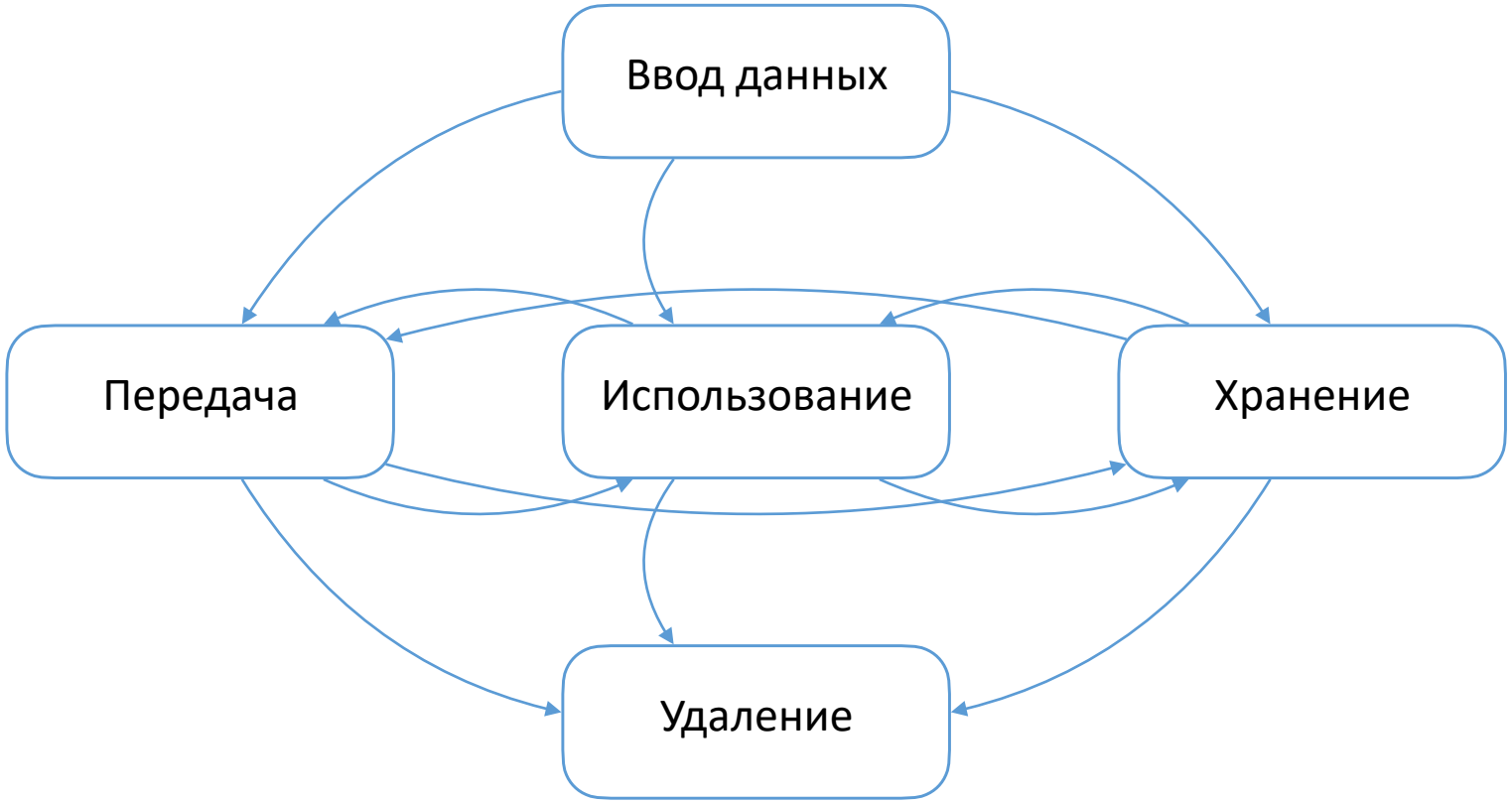
Жизненный цикл данных



Жизненный цикл данных



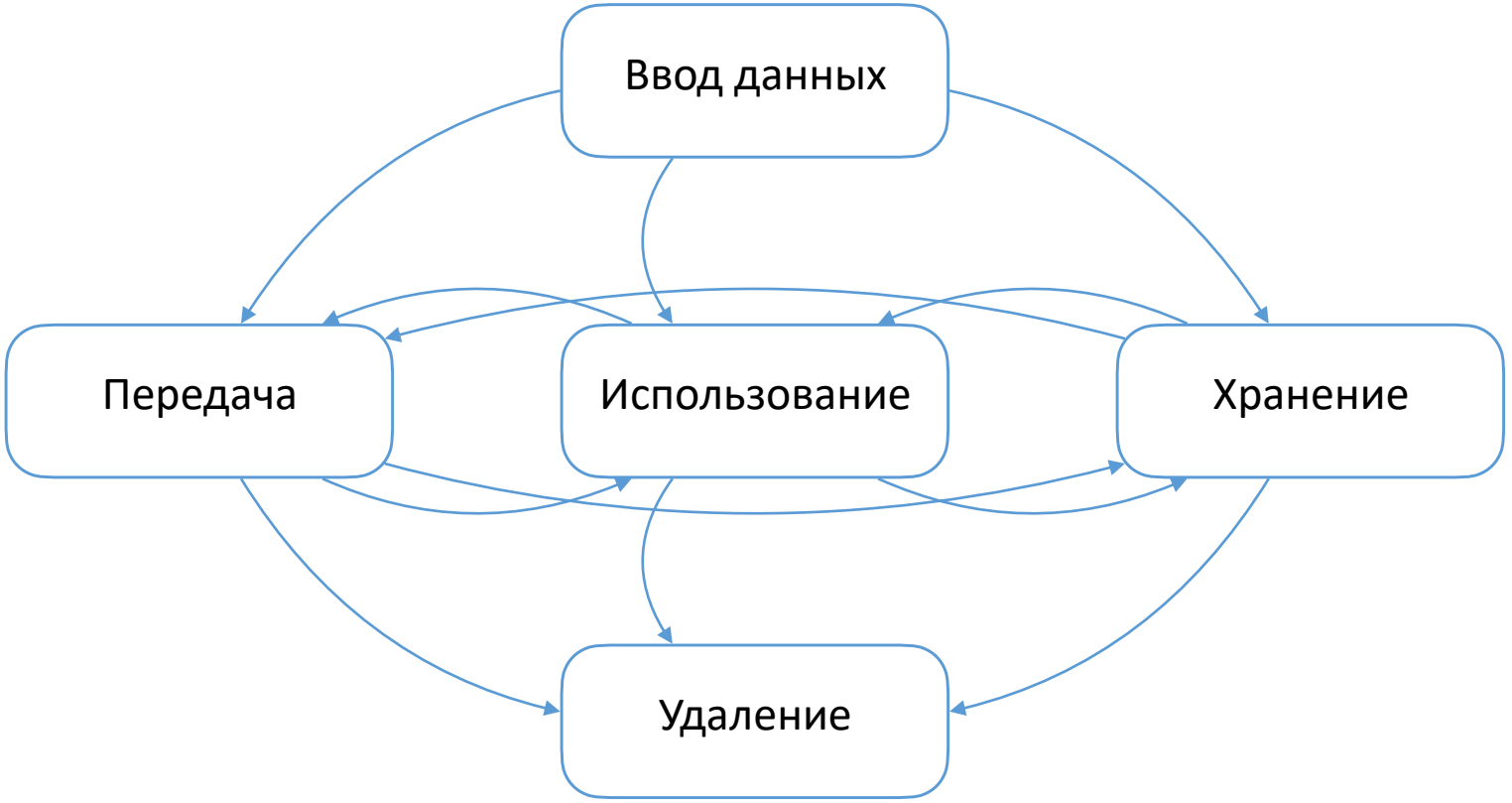
Жизненный цикл данных



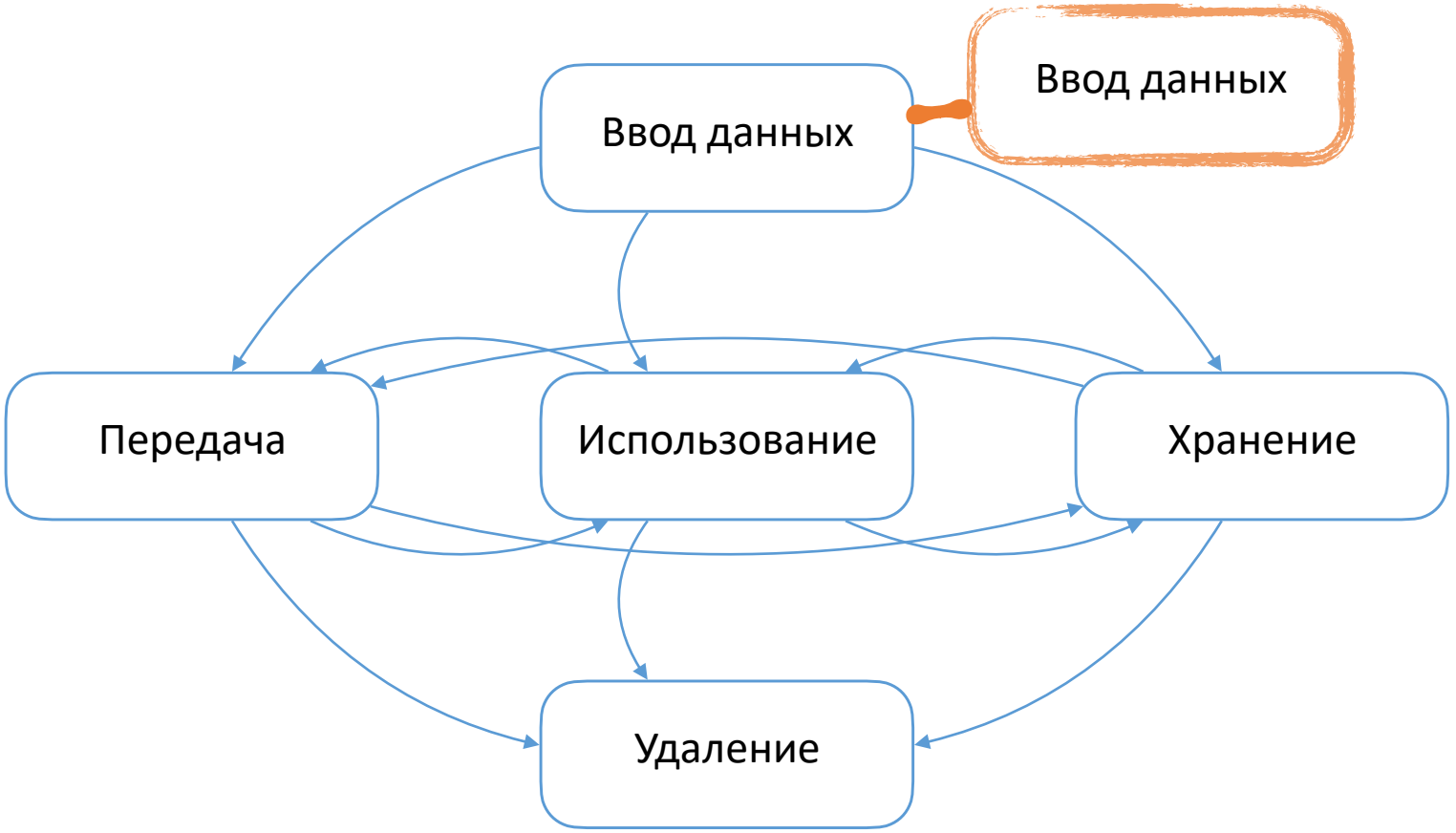
Очевидный вывод

Защита данных - это наличие возможности осуществить все переходы, определенные циклом, с отсутствием нелегитимных действий

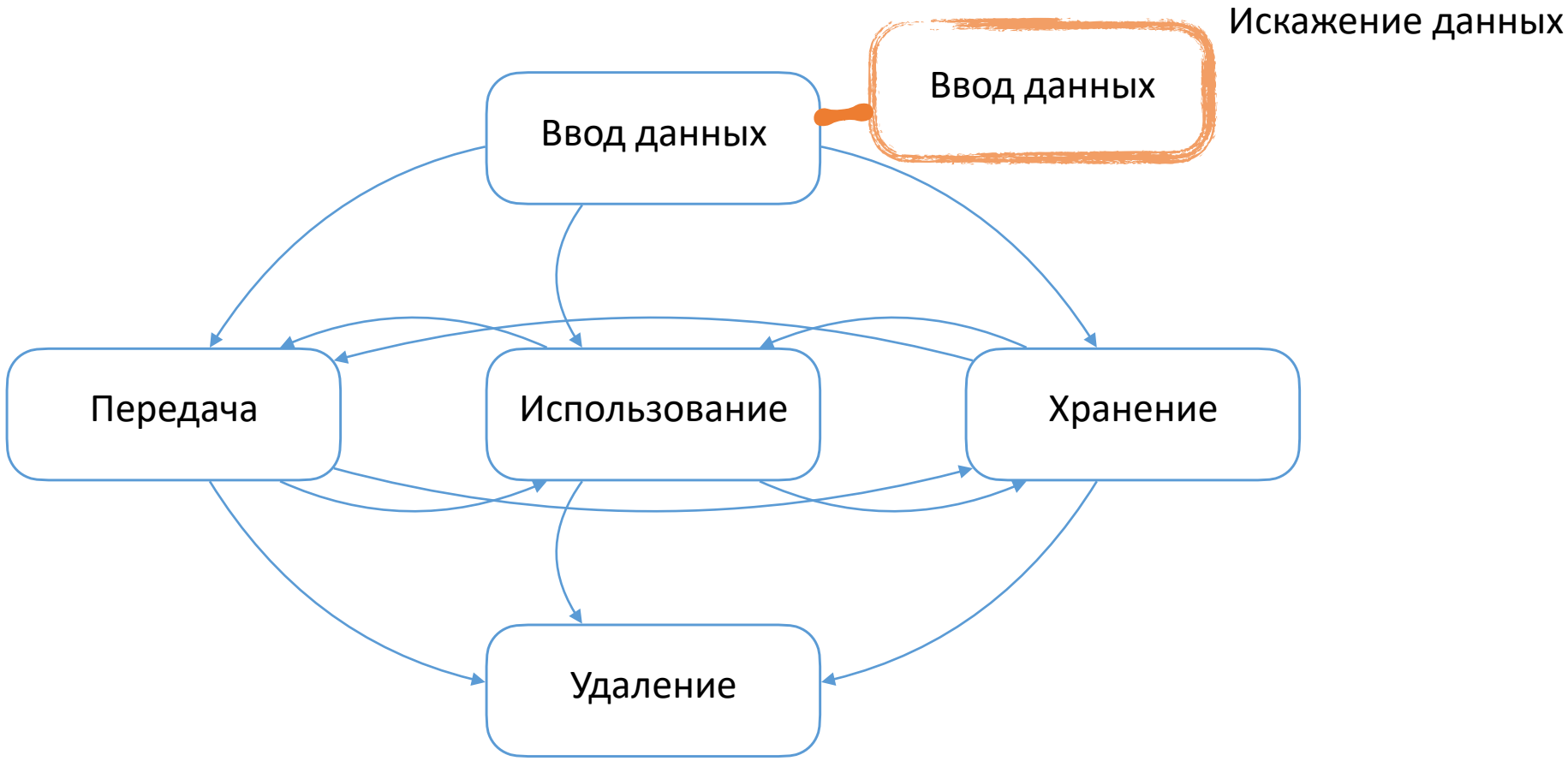
Примеры нелегетимных действий



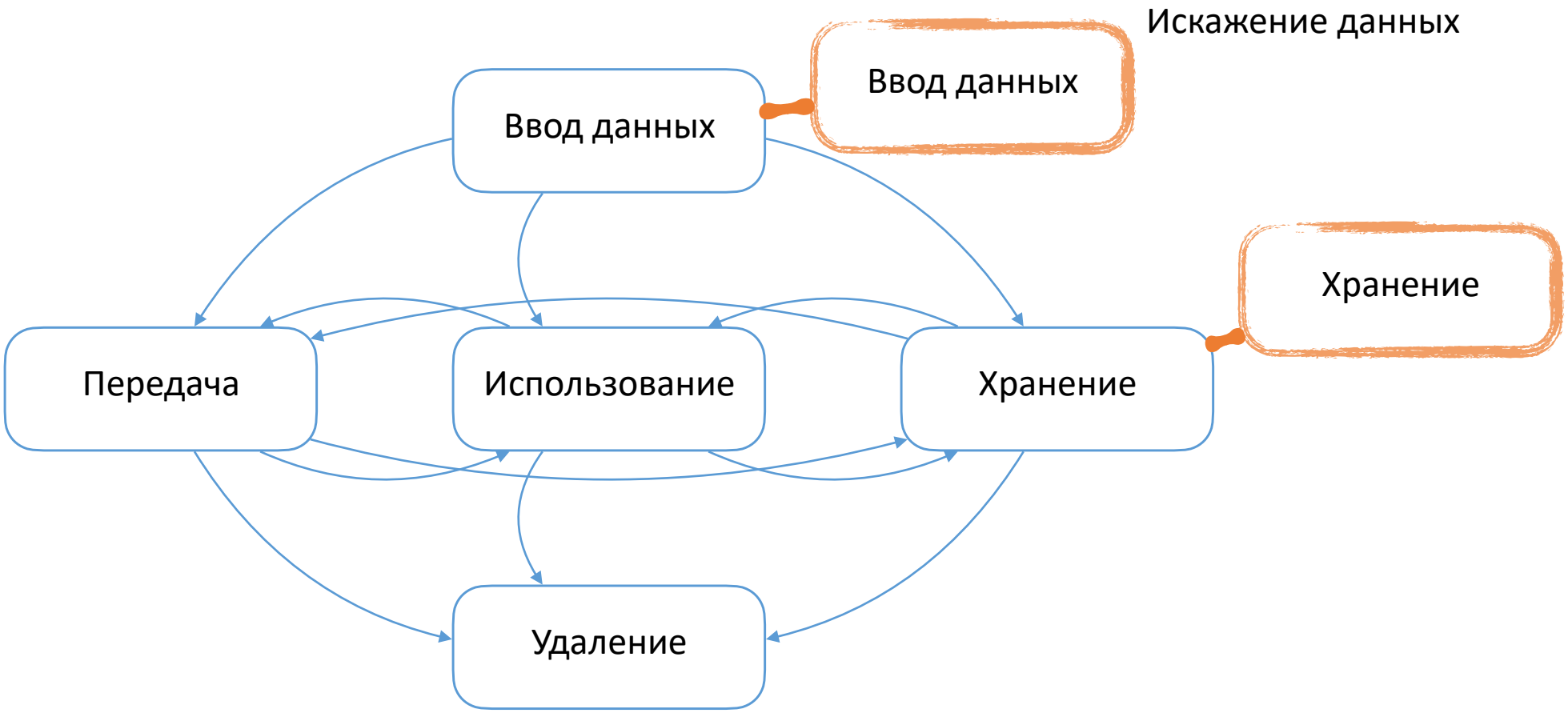
Примеры нелегетимных действий



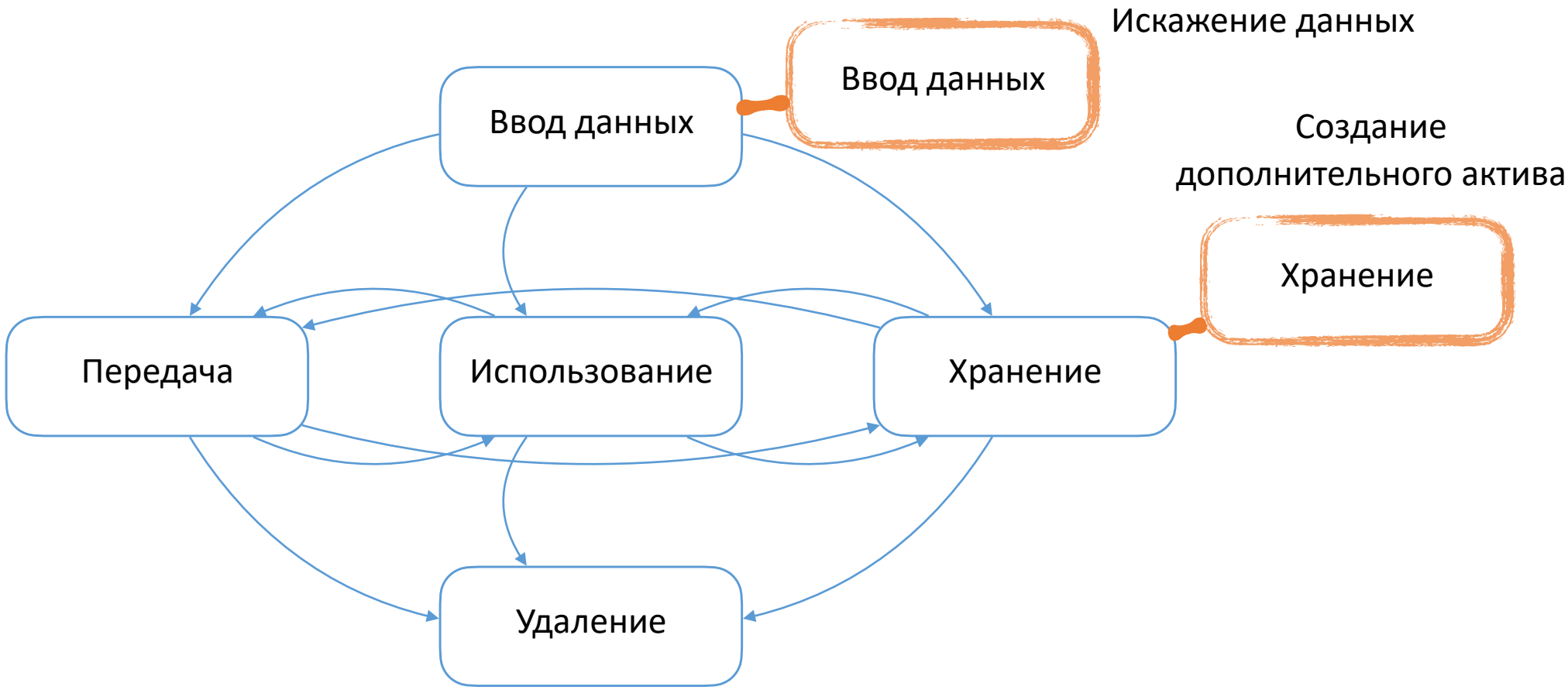
Примеры нелегетимных действий



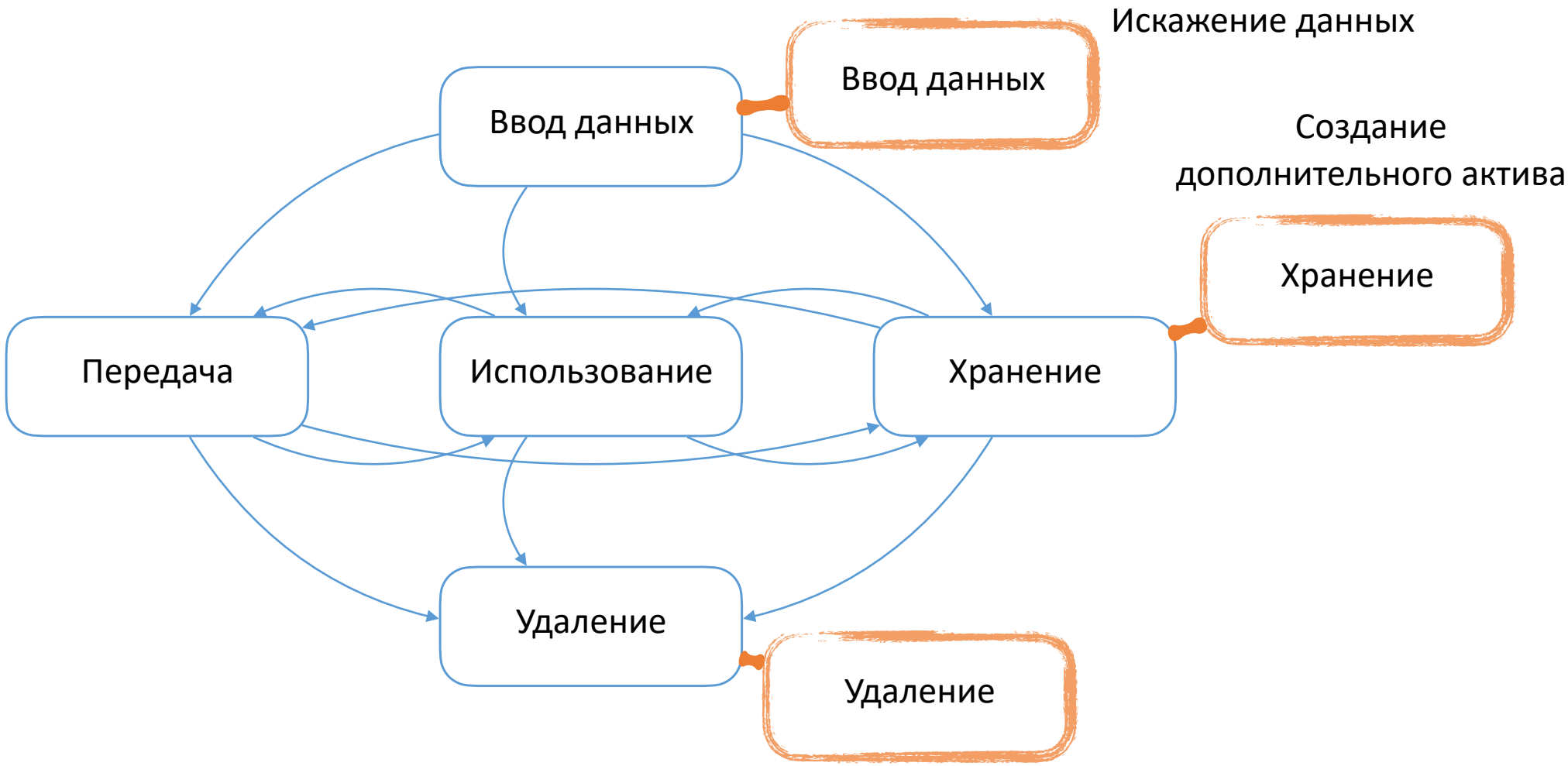
Примеры нелегетимных действий



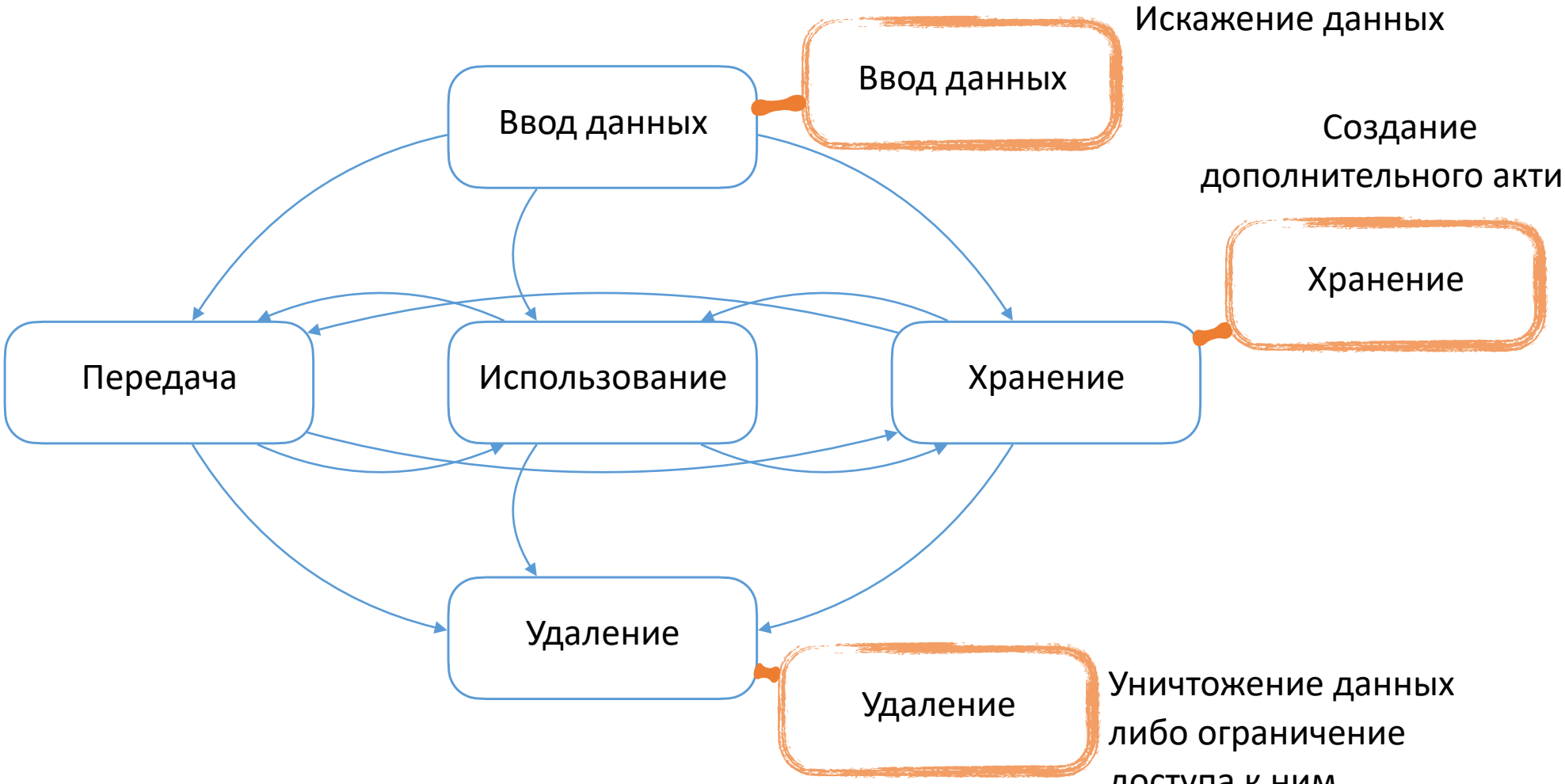
Примеры нелегетимных действий



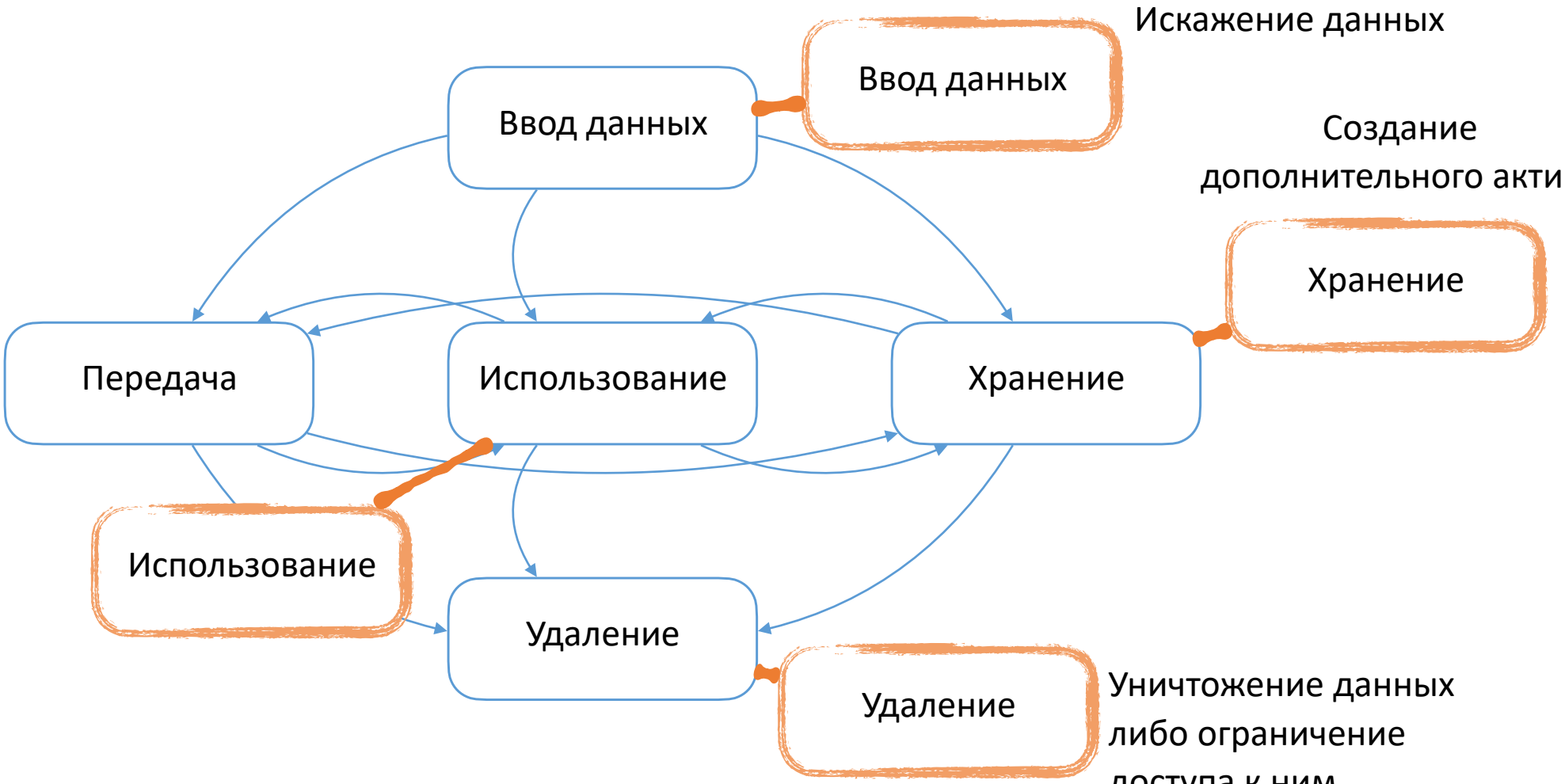
Примеры нелегетимных действий



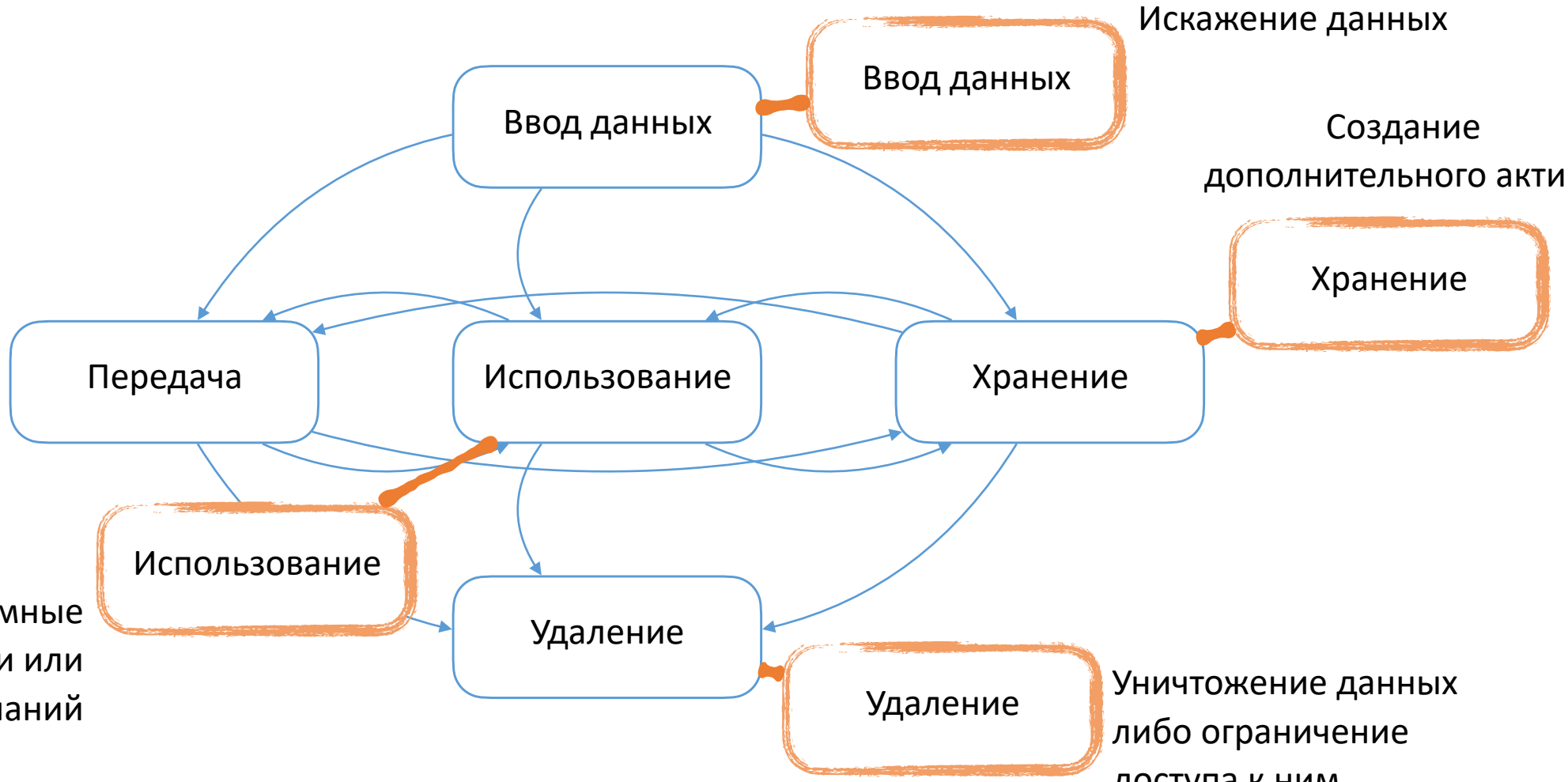
Примеры нелегетимных действий



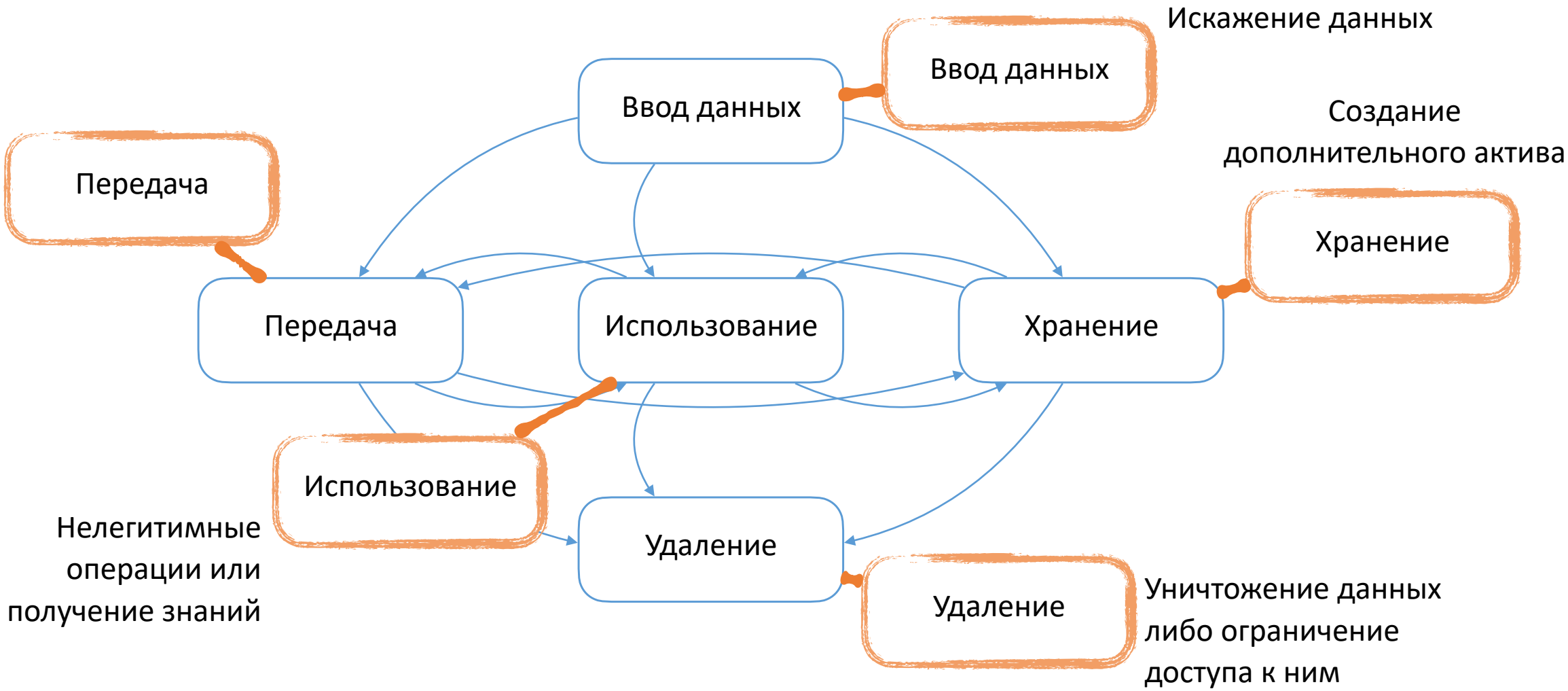
Примеры нелегетимных действий



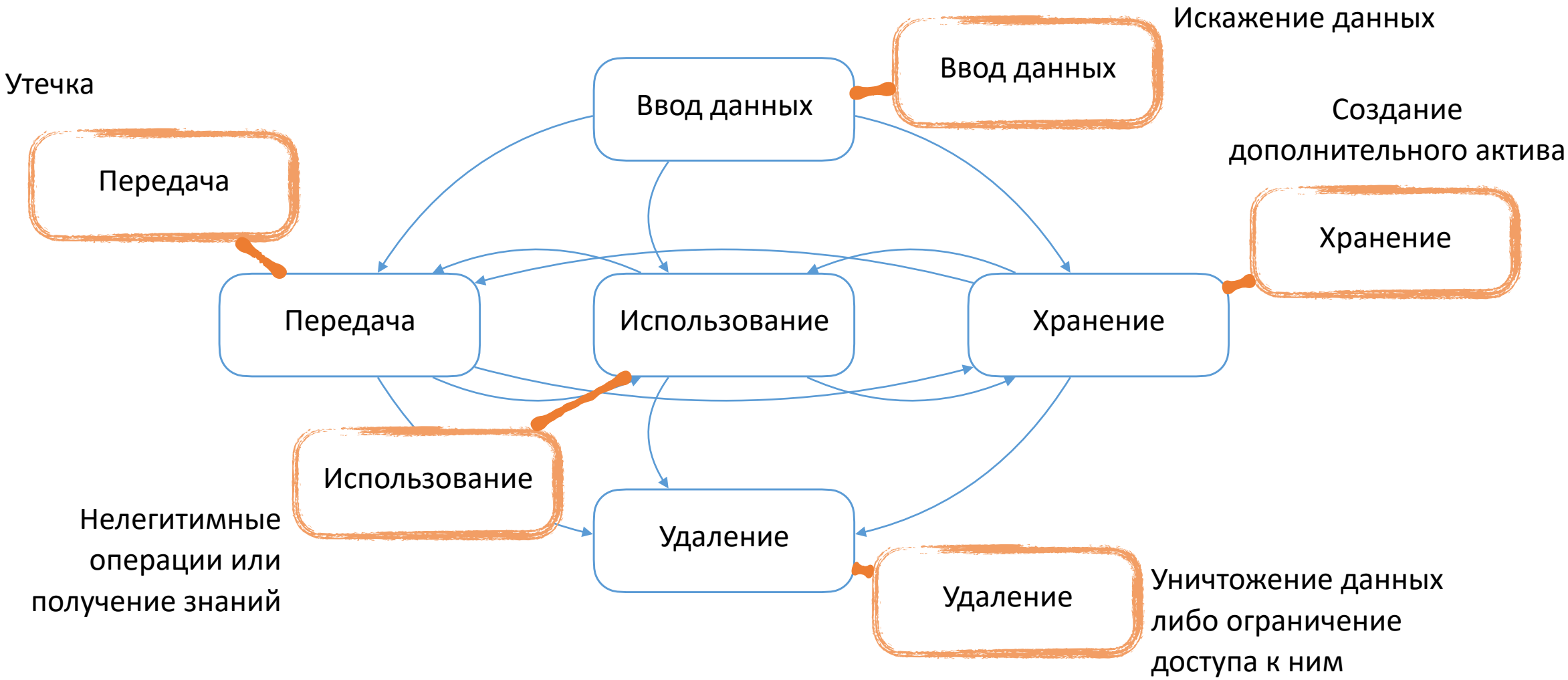
Примеры нелегетимных действий



Примеры нелегетимных действий



Примеры нелегетимных действий



Кейсы простые: ввод и удаление

1) По возможности автоматизированный ввод
2) Если ввод ручной, то принцип 4-х рук / глаз
3) Удаление должно быть надежным
4) Удаление нужно авторизовывать

Использование данных

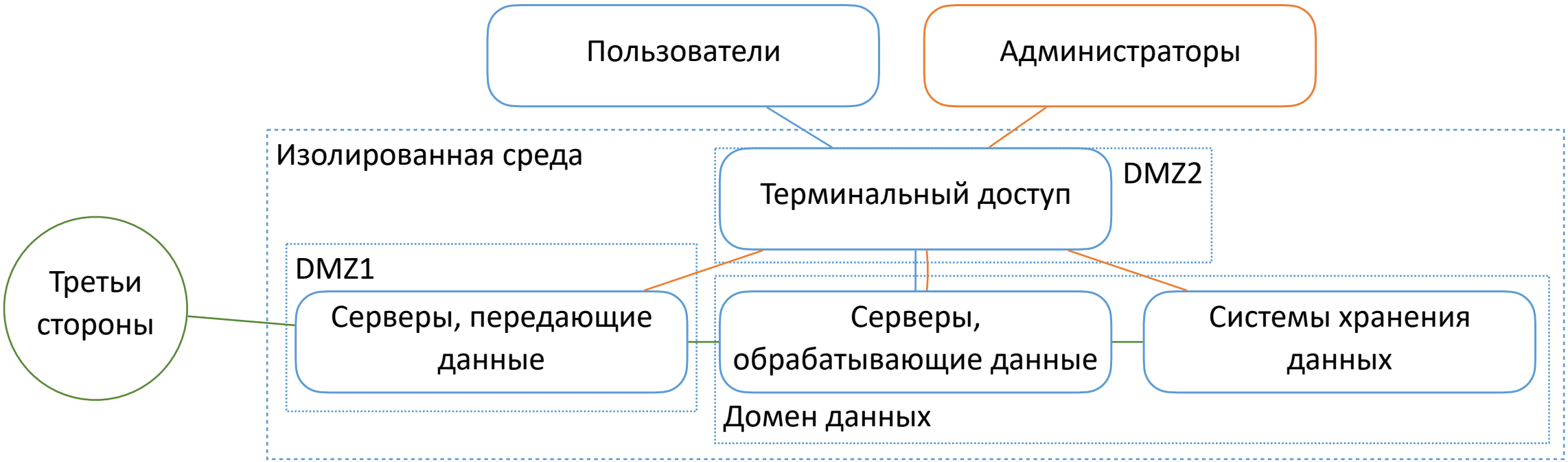
- Минимизировать использование
- Автоматически снизится потребность в передаче и хранении
- **Не забыть про контроль доступа и выгружаемых данных. На уровне прав и логов**
- Экран всегда можно сфотографировать, а хранимое в головах изложить в документе. Нужен Security Awareness
- **Потребуется создание некоторых glass-view технологий, в которых данные можно использовать, но нельзя экспортировать из организации. Либо DRM. Либо IRM. На выбор.**

Передача данных

- При экспорте данные никаким образом не защитить
- Требуется тщательный анализ на уровне договоров и технологий, какие данные каким третьим сторонам передаются
- Большая организация стала похожа на интернет: что попало к работникам, то скорее всего уже разглашено

Хранение данных

- Изолированные домены с данными выглядят действительно хорошей идеей
- Не забывать про защиту резервных копий



Интересные наблюдения

- Контролировать каналы утечки можно, но нужно их непрерывно инвентаризировать, гоняться за вендором, добиваться получения prevention функционала
- Предложенная схема недешевая, но она дешевле, чем «гоняться за красным октябрем» с администраторами и аналитиками
- Если производители DLP не начнут делать DLP вместо DLD, все уйдут в модель изолированных сред