Требования законодательства к обезличиванию данных и промышленных подход к их реализации

Михаил Комаров,
Директор по развитию бизнеса,
Решения Informatica

DIS Group

Статистика по России

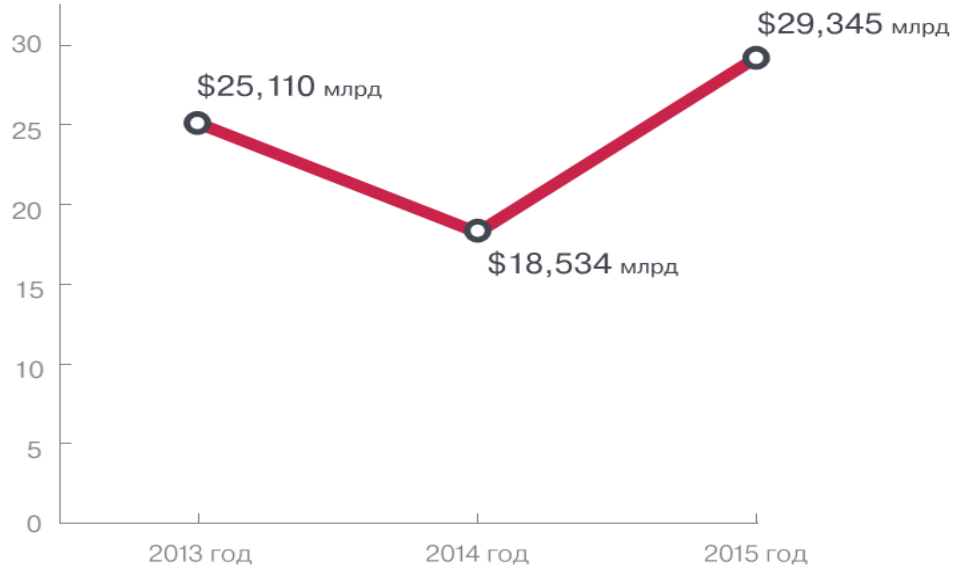
ZECURION ANALYTICS

УТЕЧКИ ИНФОРМАЦИИ 2016

Ключевые выводы

- В 2015 году зарегистрирован рекордный ущерб от утечек информации — более $29 млрд.
- Россия на 4 месте (после США, Великобритании и Канады) в мире по числу утечек (49 публичных инцидента за 2015 год).
- Финансовые данные физлиц — один из самых востребованных киберпреступниками типов информации — утекают в 19,1% инцидентов.

Рисунок 4 ▶
Убытки от утечек информации



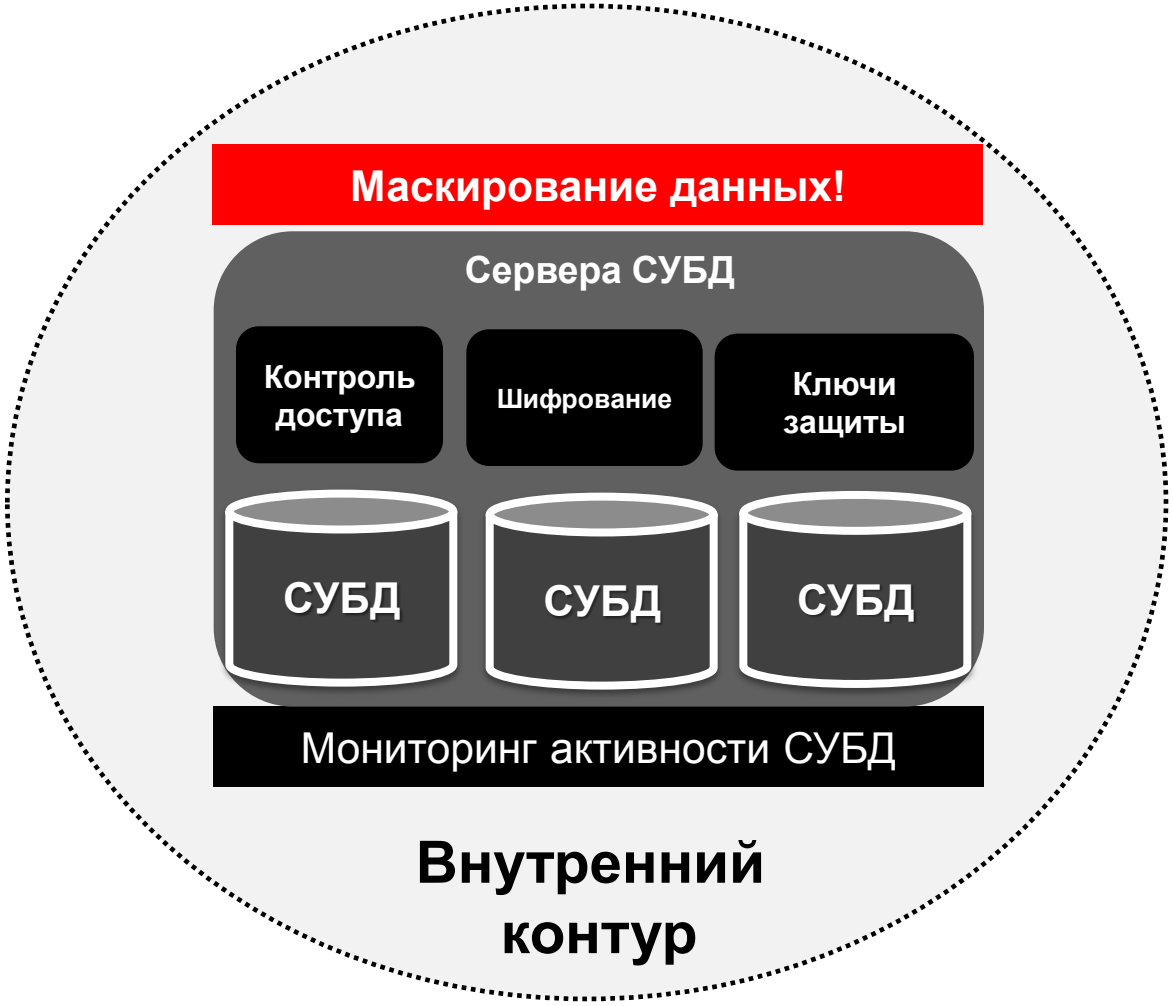
Источник: Утечки конфиденциальной информации в России и в мире. Zecurion Analytics 2016

Кто представляет опасность?

Маскирование данных

необходимый компонент системы безопасности

- Маскирование тестовых данных:
  - Тестовые среды
- Маскирование особо важных продуктивных данных на лету:
  - CRM, ERP и т.д.
- Работа с текущими политиками и устранение пробелов в информационной безопасности



"Организации должны использовать маскирование данных для защиты конфиденциальных данных от злоупотреблений инсайдеров и внешних угроз" **Gartner, Data Masking Magic Quadrant**

Требование законодательства по обезличиванию данных

Наименование документа	Краткое описание и ссылки на необходимые разделы и пункты
Закон № 152-ФЗ «О персональных данных»	Согласно Закону № 152-ФЗ персональные данные - **любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.**
Ст. 26 закона «О банках и банковской деятельности»	Согласно ст. 26 закона «О банках и банковской деятельности» к банковской тайне относится информация об операциях, счетах и вкладах клиентов и корреспондентов. По российскому законодательству кредитная организация гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

Требование законодательства по обезличиванию данных

Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность **их обработки**. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных. *

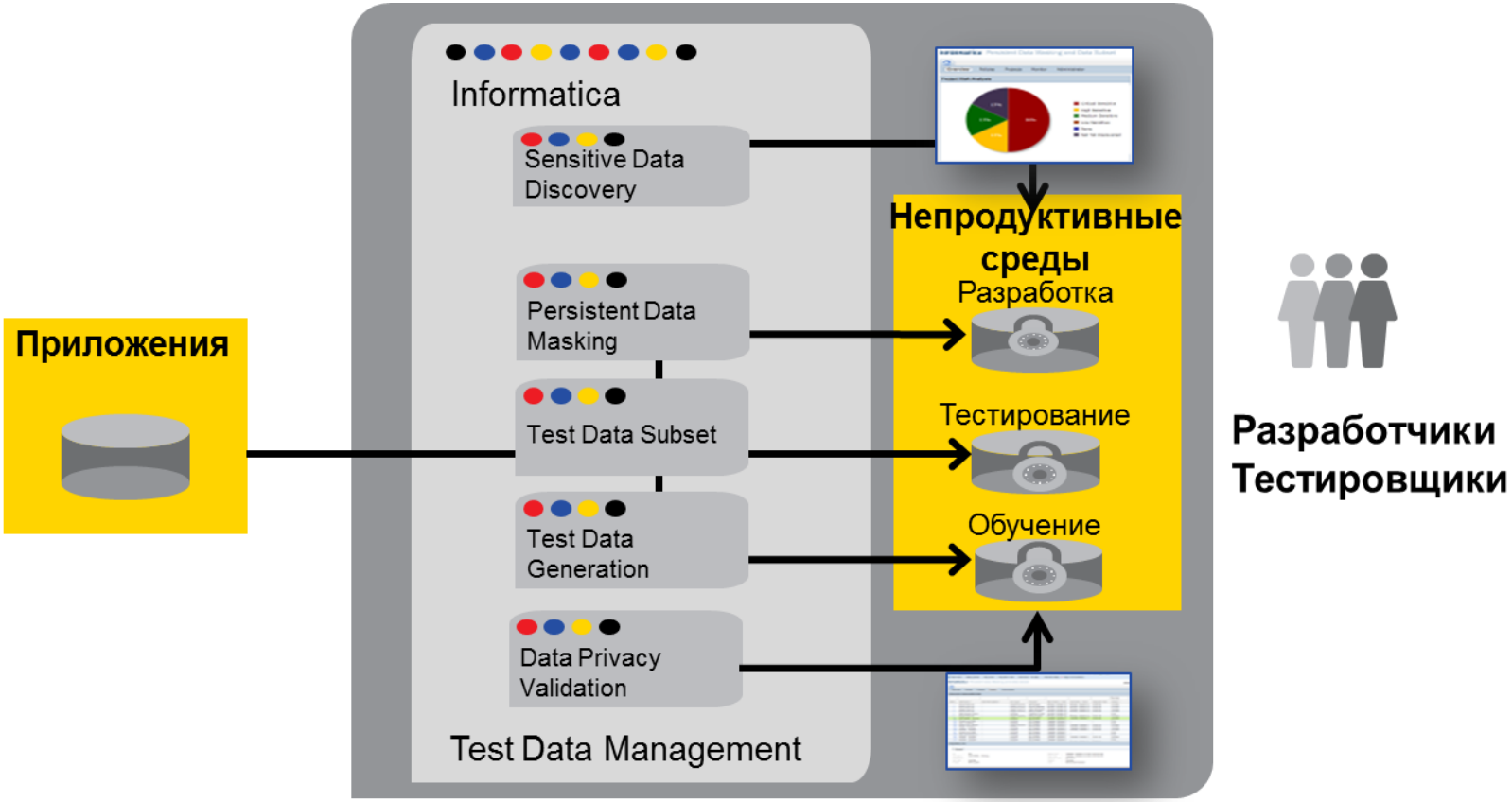
***Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 5 сентября 2013 г. N 996 г. Москва "Об утверждении требований и методов по обезличиванию персональных данных"**

Свойства обезличенных данных

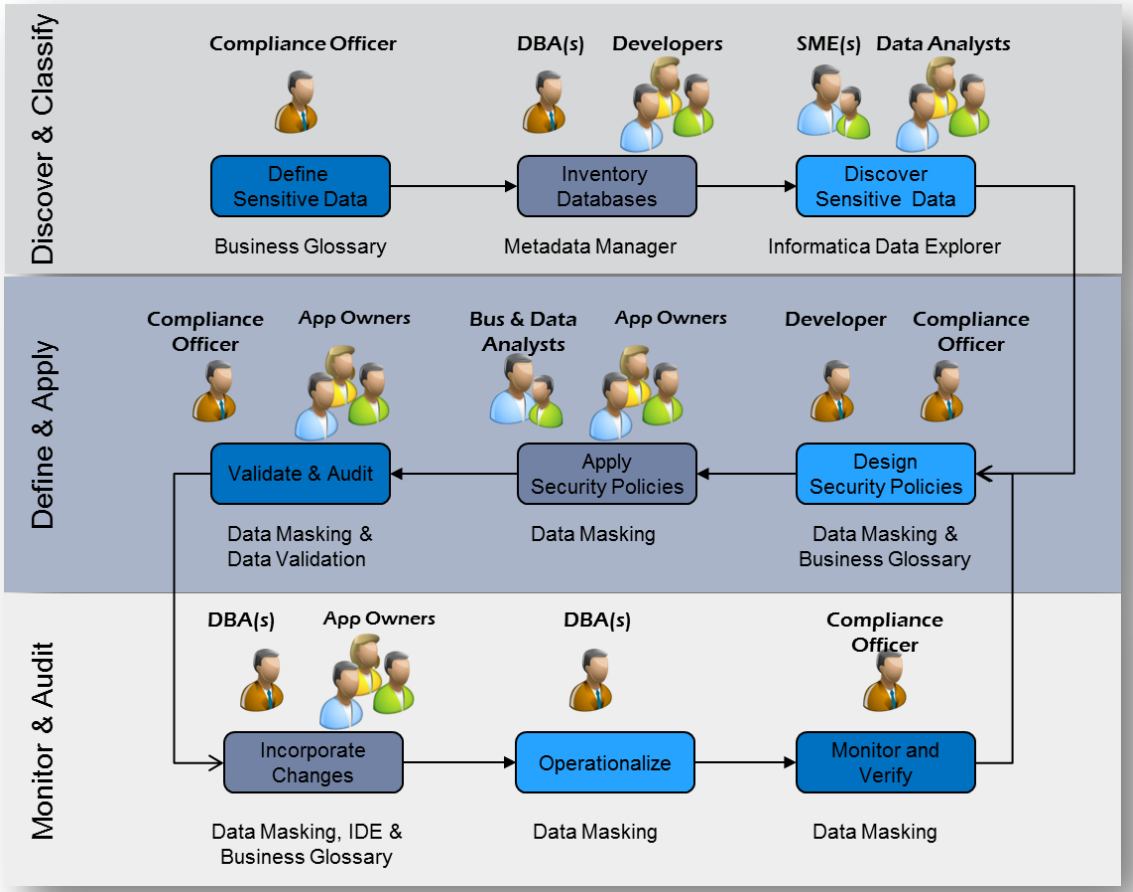
- **полнота** (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания);
- **структурированность** (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);
- **релевантность** (возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме);
- **семантическая целостность** (сохранение семантики персональных данных при их обезличивании);
- **применимость** (возможность решения задач обработки персональных данных, стоящих перед оператором, осуществляющим обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ (далее - оператор, операторы), без предварительного деобезличивания всего объема записей о субъектах);
- **анонимность** (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).


И ТАК СОЙДЕТ!

Промышленная платформа для обезличивания данных – Informatica TDM



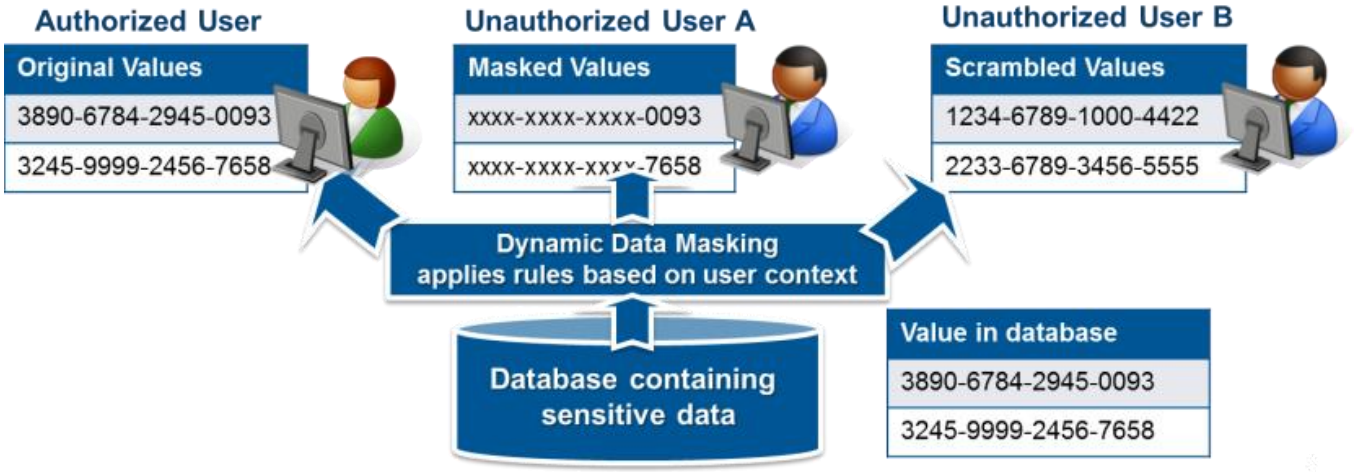
Методология Informatica по обезличиванию данных



Динамическое маскирование

Защита данных в продуктивных средах

- Informatica Dynamic Data Masking защищает критически важную информацию пользователей и приложений, которые не должны иметь доступ к ней
- Обеспечивает для каждого пользователя доступ к информации в соответствии с данными об идентификации, ролью и областью ответственности без изменения приложений и баз данных
- Блокирует доступ к данным полностью или частично по правилам безопасности



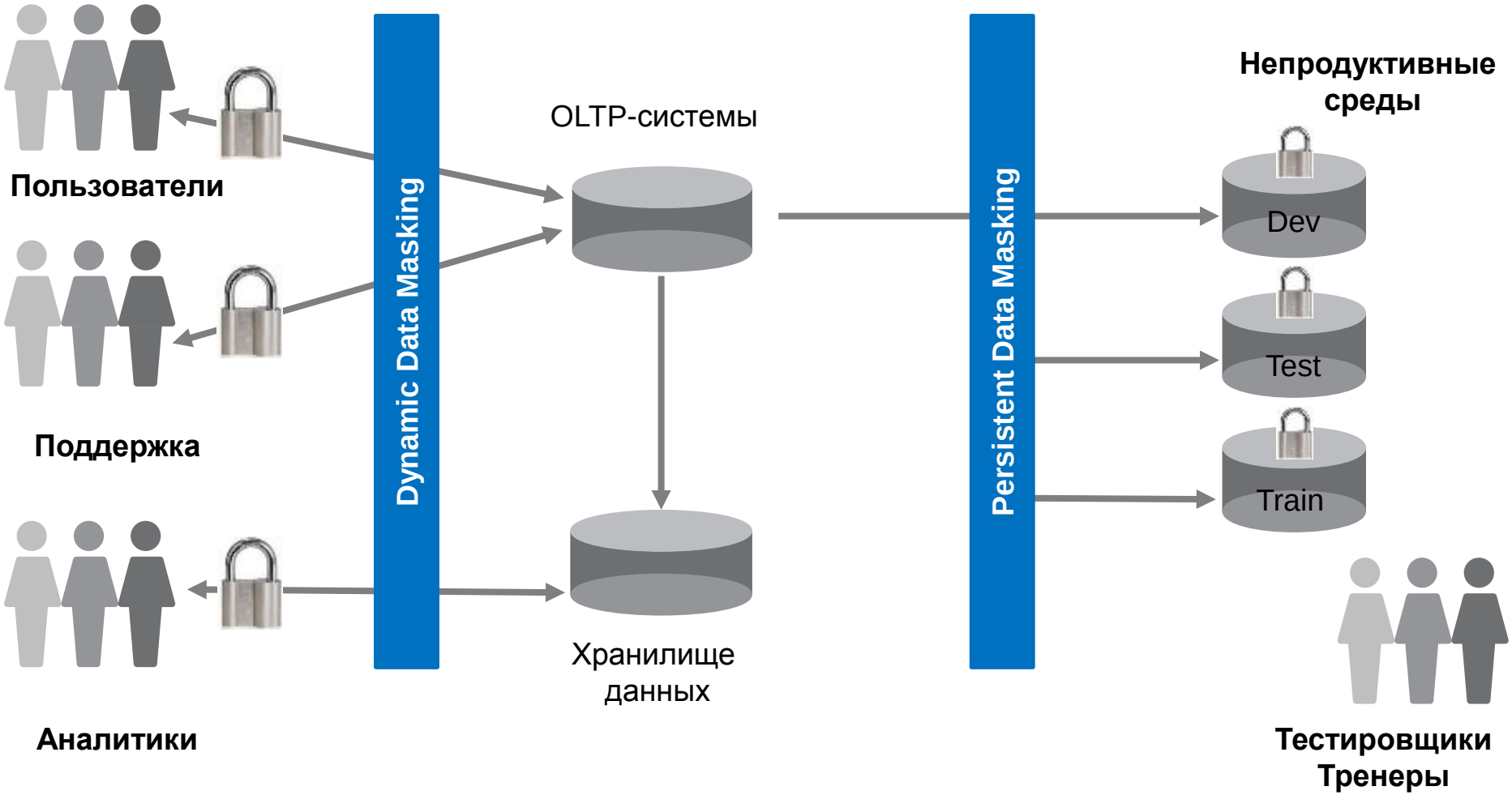
Какие данные нужно маскировать в реальном времени?

DIS

- Данные VIP клиентов
- Контактная информация
- Финансовая информация
- Коммерческая тайна
- Любая другая чувствительная информация
- Информация, к которой имеют доступы разные группы пользователей
- Любые клиентские данные для иностранных компаний

Обезличивание данных

Защита промышленных и тестовых данных



DIS

СБЕРБАНК
Всегда рядом

Результаты внедрения

- Трудоемкость обезличивания АС снижена **с 50 до 3 чел-дней**
- Трудоемкость проверки обезличенных данных сотрудниками информационной безопасности снижена **с 10 до 3 чел-дней**
- АС «Обезличивание» внедрена в **промышленную эксплуатацию**
- Разработаны карты обезличивания **для более чем 60АС** с различными типами БД

Спасибо за внимание!

mk@dis-group.ru