

Data Mask: универсальное решение по маскированию данных

Данные в непродуктивной среде – основной риск утечки

Непродуктивные данные:

Представляют собой большую зону риска

В среднем 8-12 копий для каждого продуктивного источника

Приводят к появлению разрозненных источников данных

Источники защищены множеством инструментов и процессов

Постоянно растут

И со временем меняются



Традиционная инфраструктура



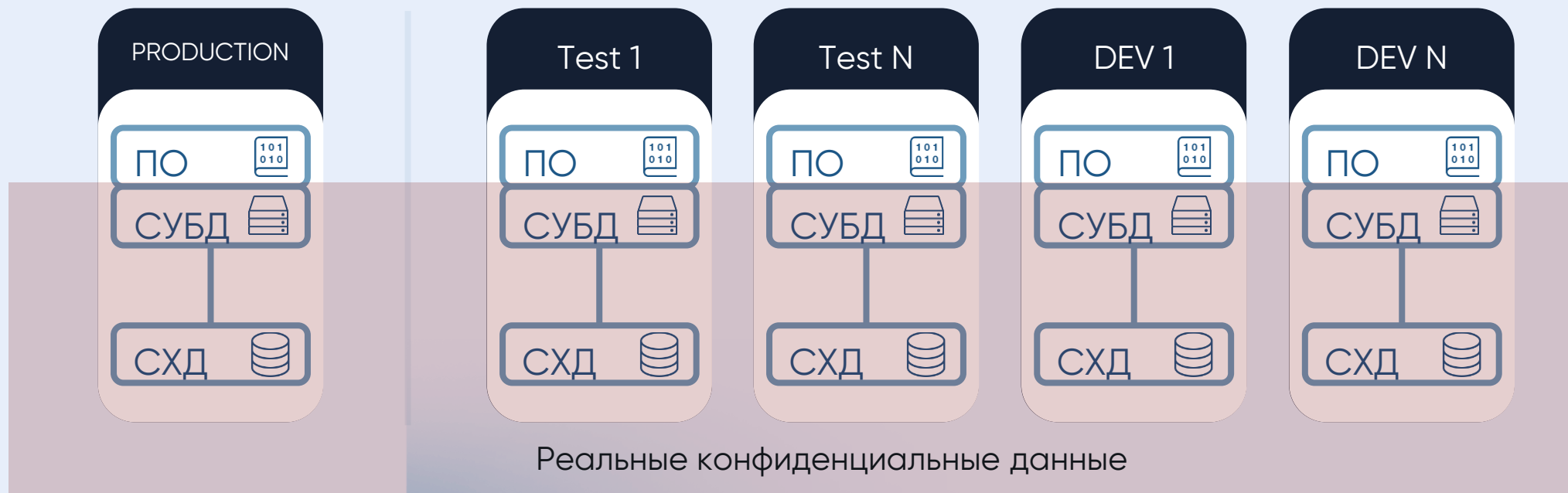
Риск утечки данных



Затраты на защиту

Продуктивная среда

Непродуктивные среды



20%

Продуктивные
данные

80%

Непродуктивные
данные

Инфраструктура с маскированием

Во всех 10 копиях каждой базы данных для критически важных приложений находятся замаскированные данные

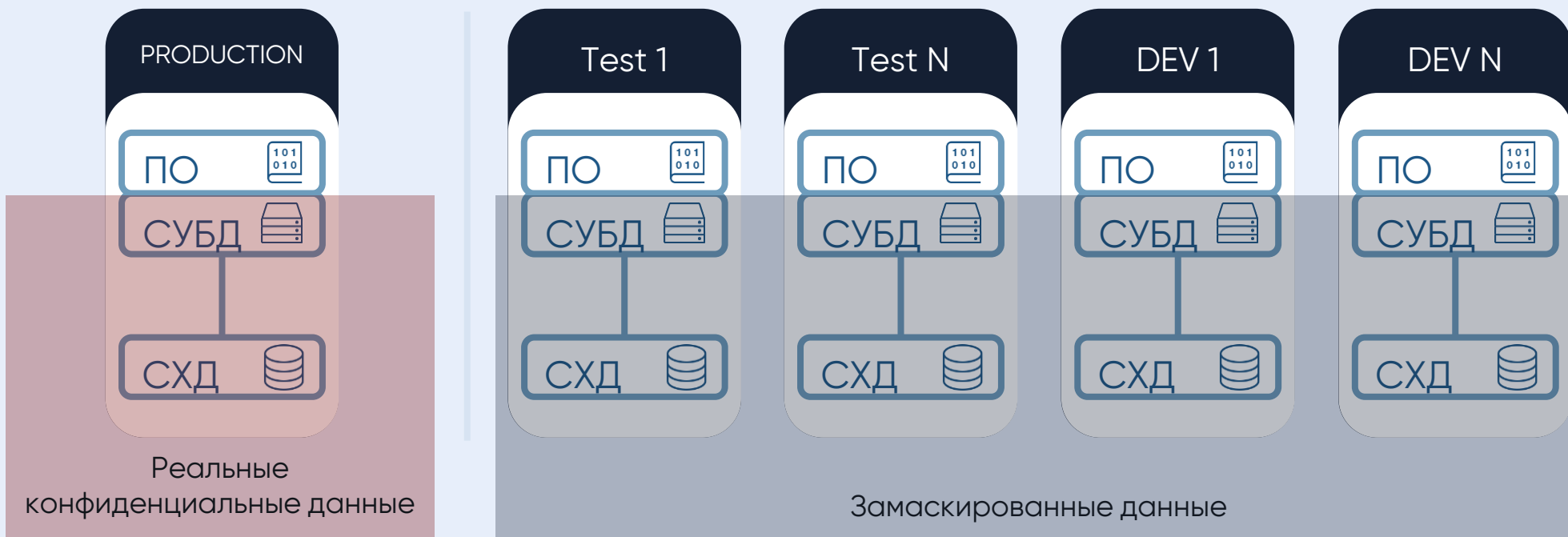
Маскированные данные максимально похожи на оригинальные. При этом непродуцированные среды остаются полностью функциональными и реалистичными



Толерантность к утечкам



Не требует затрат на защиту



Комплексный подход к безопасности



Задачи бизнеса

- Соблюдение законодательства в области персональных данных
- Уменьшение сроков разработки, как следствие экономия ресурсов и максимизация прибыли
- Возможность безопасной аналитики Big Data, как на стороне подрядчика, так и внутри организации



Задачи ИТ

- Сокращение времени и трудозатрат на создание и обновление сред разработки и тестирования, что увеличивает скорость разработки
- Минимизация ошибок при разработке нового продукта, так как в тестовой среде использована реальная база данных с сохранением логики, но без конфиденциальной информации



Задачи ИБ

- Сокращение времени и трудозатрат на категорирование информации при составлении ролевых моделей доступа к данным
- Повышение безопасности данных в периметре организации
- Уменьшение шансов риска утечки конфиденциальной информации

Маскирование данных

Реалистичность

Необратимость

Целостность

Однородность

Маскирование всех источников

– Одинаковые правила и алгоритмы

Целостное Маскирование

– Одинаковое маскирование всех источников

Различные алгоритмы маскирования

- По словарю с учетом того, от какого лица, пола формулировки в документе
- Посимвольная замена
- На основе контрольных знаков (ИНН, ОГРН и пр.)
- Уникальные алгоритмы маскирования «под клиента»
- Замена чувствительных данных на константу

На что похожи маскированные данные

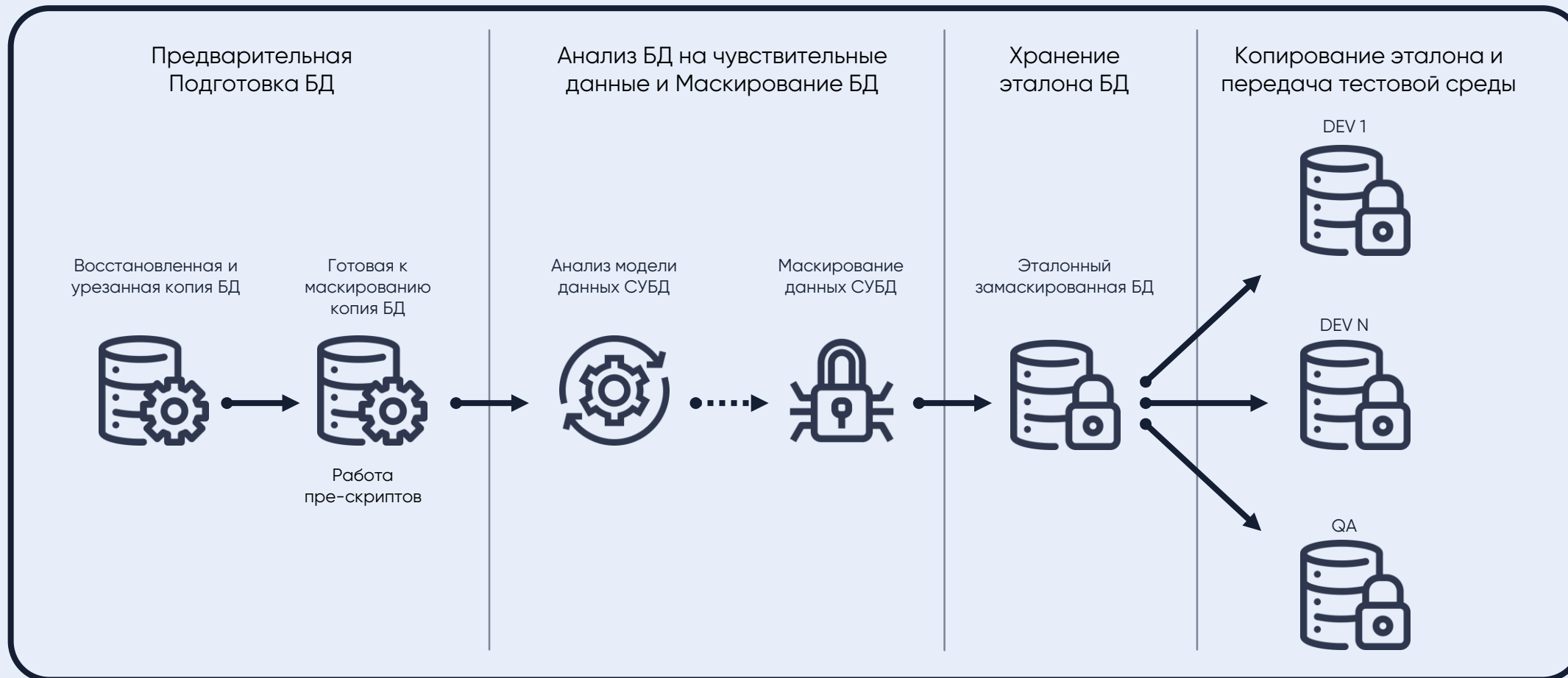
Name
Андрей Воронин
E-mail
voronin@corp.ru
Credit Card
4111-6420-7553-1464



Name
Никита Пушкин
E-mail
pyshkin@corp.ru
Credit Card
4111-4325-2277-8300

Процесс предоставления тестовых сред с учетом маскирования данных

Этапы формирования тестовых сред (ТС) с учетом маскирования



Полный цикл создания ТС при актуализации БД до состояния продуктива

Особенности процесса маскирования



Возможность удаления ненужных таблиц и полей из процесса маскирования.



Пропуск отдельных символов. Например: первые проверочные 4 символа в ИНН – это расположение регионов, эти данные не чувствительны, поэтому остаются, а остальные заменяются.



Вернуть обезличенные данные к их изначальному виду невозможно.



Словари для маскирования предоставляются вместе с продуктом, а также есть возможность их генерации по запросу клиента



Два возможных варианта маскирования:

- Работа с копией (база данных копируется и маскирование выполняется в ней)
- Данные маскируются «на лету», результат вставляется в новую БД



Преимущества решения

Возможность одновременной обработки различных баз данных в рамках одного процесса.

Консистентность данных из разных СУБД в рамках одного заказчика.

Уникальная схема маскирования для каждого заказчика.

Запуск маскирования как в ручном, так и в автоматическом режиме.

Параллельное обезличивания одной таблицы.

Предпросмотр результатов маскирования и тестовый прогон процесса обезличивания по колонке .

Поддержка большого количества СУБД: Postgres, Oracle, MS SQL, Maria DB, и др.

Возможность миграции данных из одного типа СУБД в другой.

Нужна консультация?

 info@dataprotect.ru

 dataprotect.ru