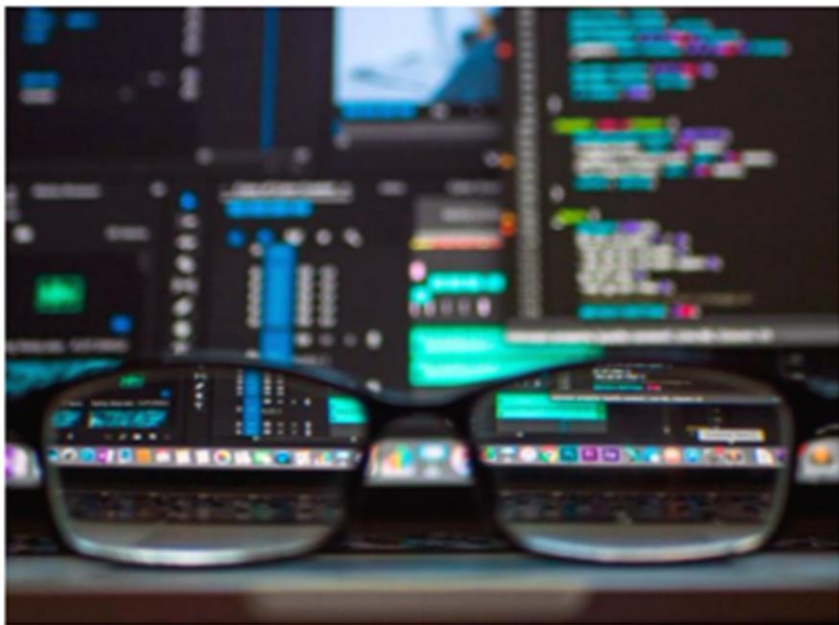




SecretTechnologies

Системы поиска и маскирования данных ДатаКамуфляж (от ДатаПротект)

Утечки данных?



В первом квартале 2023 года произошла 31 крупная российская утечка, данные которых, так или иначе, попали в открытый доступ; это вдвое больше числа утечек за первый квартал прошлого года, а суммарный объем утекших данных составил 118 миллионов уникальных записей, что в 2,3 раза больше, чем за аналогичный период прошлого года, сообщает российский сервис разведки утечек данных и мониторинга даркнета DLBI (Data Leakage &

Breach Intelligence) во вторник.

Позавчера в ограниченном доступе появились три SQL-дампа, содержащие данные CRM/CMS-системы предположительно «Школы управления СКОЛКОВО» (skolkovo.ru). 🔥

<https://www.tadviser.ru>

<https://www.tadviser.ru>

<https://t.me>

Данные в непродуктивной среде – основной риск утечки

Непродуктивные данные:

Представляют собой большую зону риска

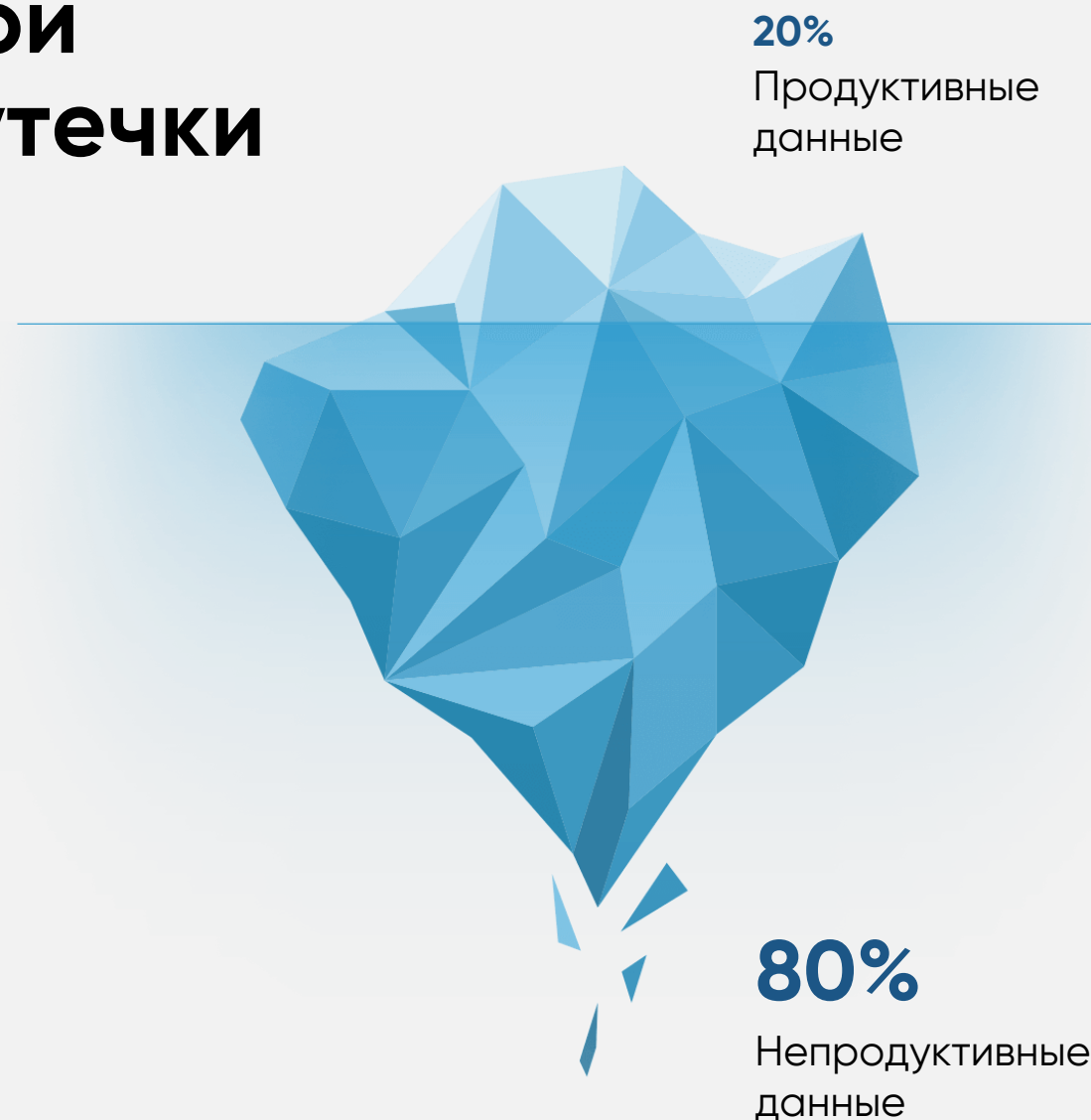
В среднем 8–12 копий для каждого продуктивного источника

Приводят к появлению разрозненных источников данных

Источники защищены множеством инструментов и процессов

Постоянно растут

И со временем меняются



Традиционная инфраструктура



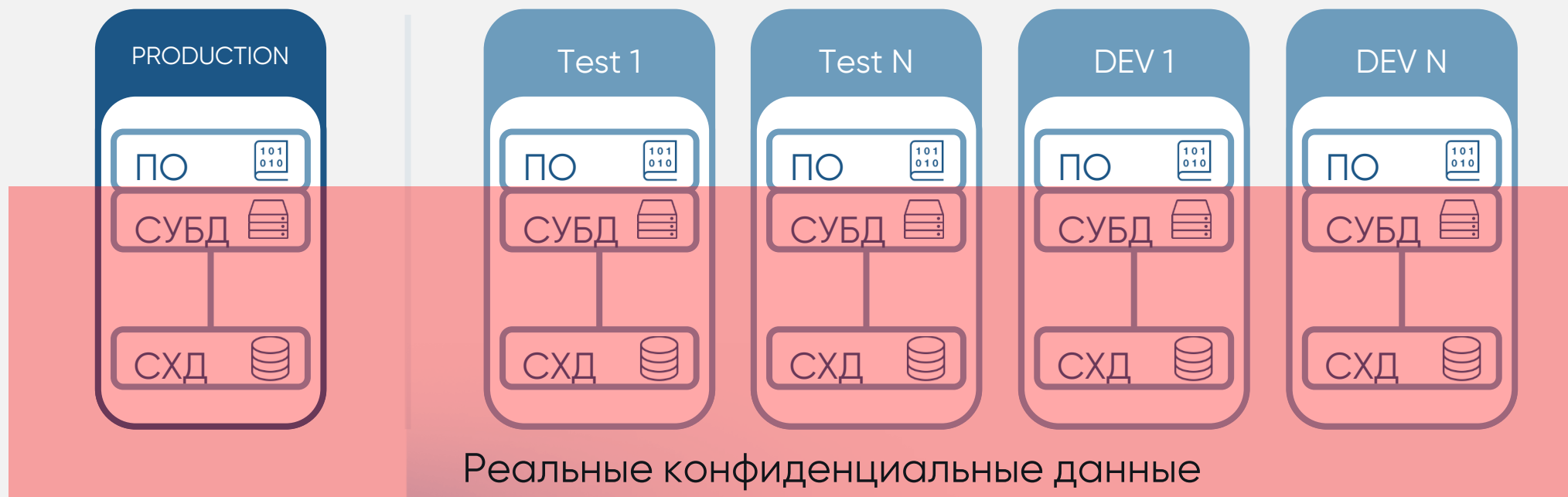
Риск утечки данных



Затраты на защиту

Продуктивная среда

Непродуктивные среды



20%

Продуктивные
данные

80%

Непродуктивные
данные

Сколько стоит утечка?

Минцифры готовит новую версию законопроекта об оборотных штрафах за утечку персональных данных

<https://digital.gov.ru>

Опубликовано:
12 июля 2022

«Оборотные штрафы, на введении которых настаивает Минцифры, будут исчисляться в процентах от выручки компаний. Так, оборотный штраф в 1% для компании с выручкой в 100 млрд руб. составит 1 млрд руб.»

2022 Яндекс Еда

данные клиентов, с именами и фамилиями, номерами телефонов, адресами доставки и комментариями.

49 441 507 (49,4 млн) строк

Источник: https://www.anti-malware.ru/analytics/Threats_Analysis/Yandex-Eda-Leak-Threat

Оборот компании – 356,2 млрд ₽

Штраф – 3,562 млрд ₽

Затраты на защиту данных компаний Российской Федерации по результатам 2021 года оцениваются в 185,9 млрд руб.

Комплексный подход к безопасности



ИДЕНТИФИЦИРОВАТЬ

Обнаружение
конфиденциальных данных
и создание профиля риска
для всего предприятия



ЗАМАСКИРОВАТЬ

Применение маскирования
в автоматическом
или ручном режиме



УНИКАЛИЗИРОВАТЬ

Уникализация баз данных
методом внедрения
«изотопных меток»

На что похожи маскированные данные

Name
Андрей Воронин

E-mail
voronin@corp.ru

Credit Card
3233-4123-8211-6723



Name
Никита Пушкин

E-mail
pushkin@corp.ru

Credit Card
3233-1123-0291-9074

Маскирование данных

- ✓ Реалистичность
- ✓ Целостность
- ✓ Необратимость
- ✓ Однородность

Маскирование всех источников

- Одинаковые правила и алгоритмы

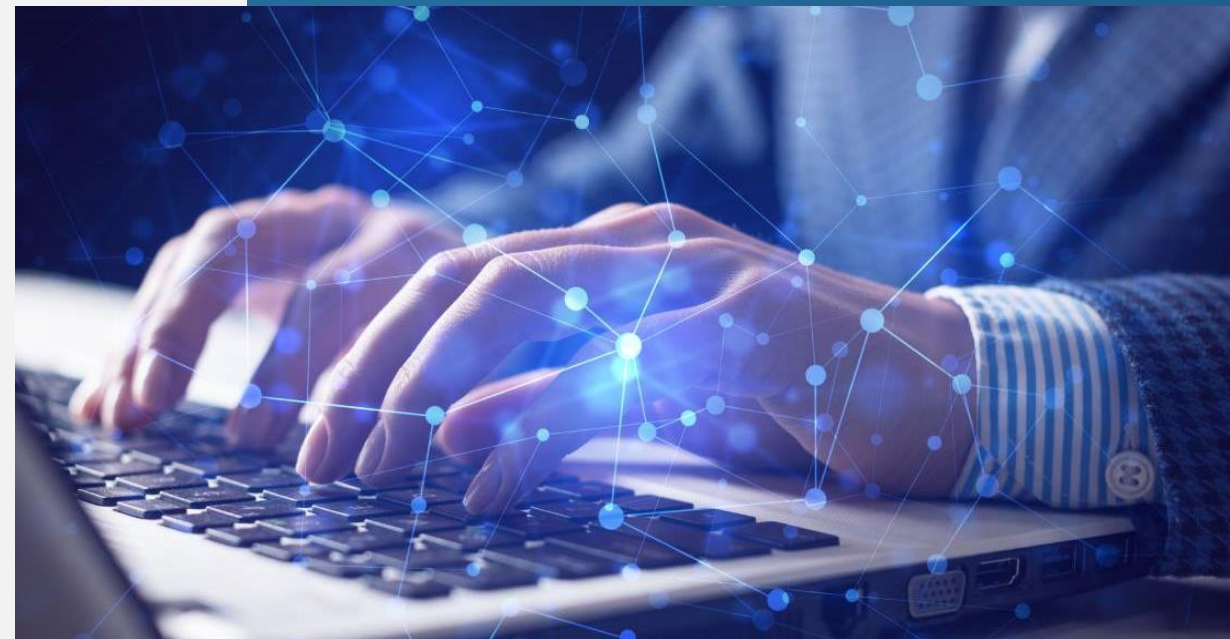
Целостное Маскирование

- Одинаковое маскирование всех источников

Маскирование по словарю

- Простой метод маскирование
- Необратимо

ORACLE		SQL Server		ORACLE		SQL Server	
Таблица заявителей		Таблица работников		Таблица заявителей		Таблица работников	
ID	Имя	ID	Имя	ID	Имя	ID	Имя
1	Иван	4	Сергей	1	Михаил	4	Виктор
2	Анна	5	Роман	2	Елена	5	Фёдор
3	Антон	6	Иван	3	Дмитрий	6	Михаил



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

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, непроизводственные среды остаются полностью функциональными и реалистичными



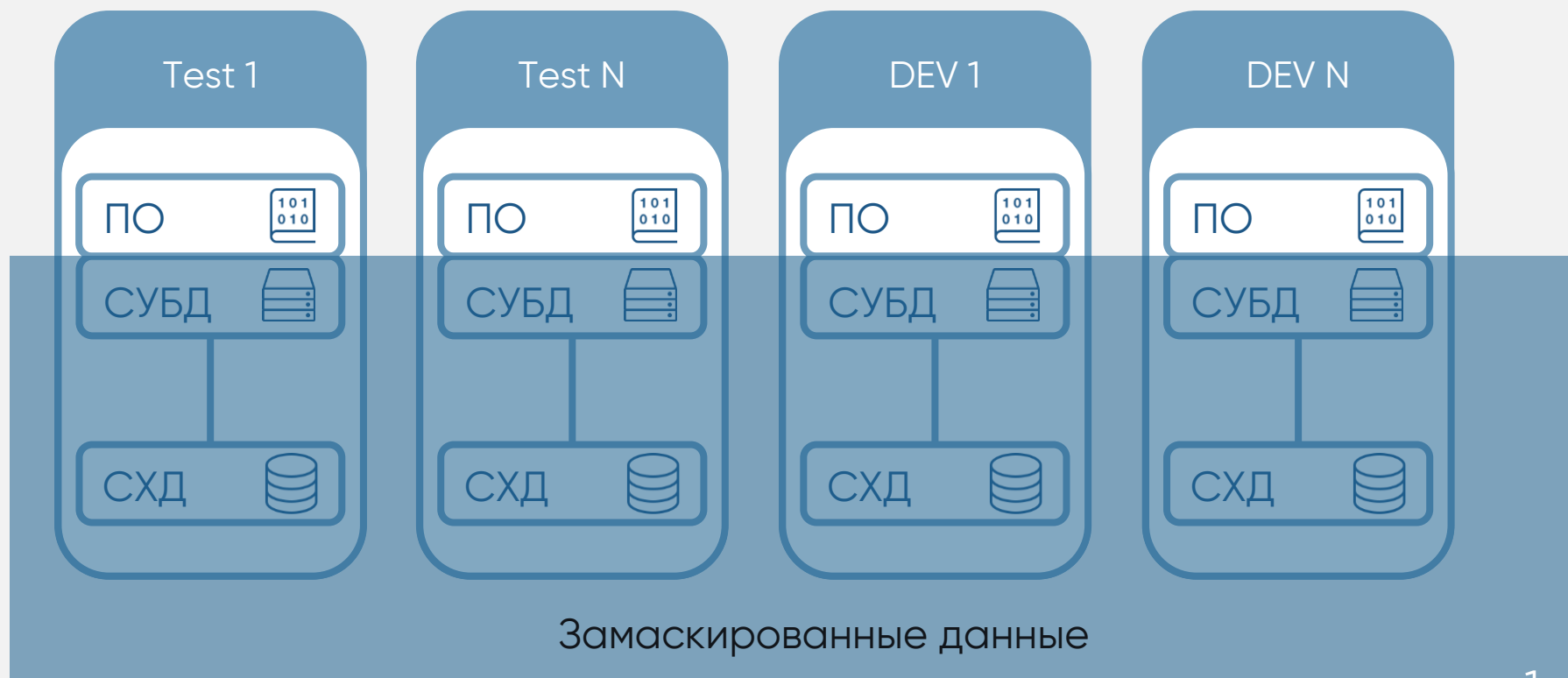
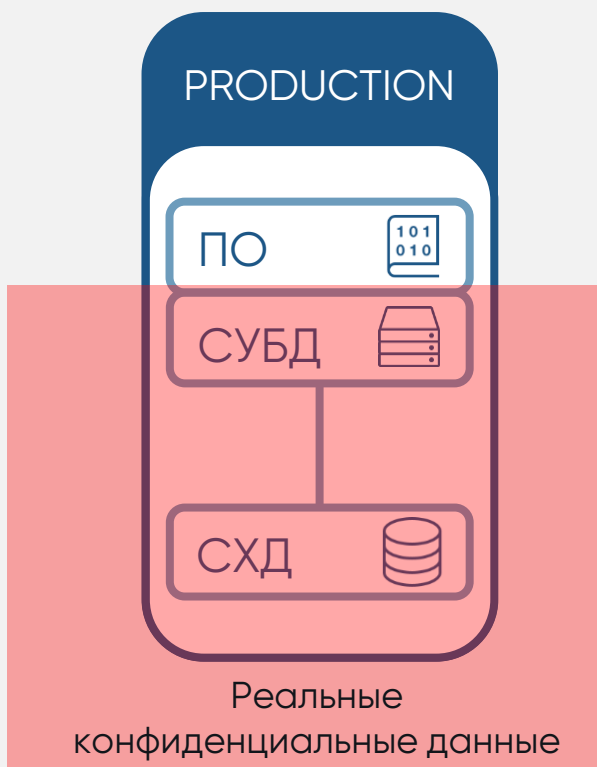
Толерантность к утечкам



Не требует затрат на защиту

Продуктивная среда

Непродуктивные среды



Наш опыт

- Успешное внедрение систем маскирования и виртуализации БД
- Разработка и внедрение собственной системы валидации данных
- Разработка и внедрение собственной систем контроля изменений в БД
- Разработка и тестирование системы поиска данных на основе машинного обучения ML
- Разработка собственных алгоритмов поиска данных
- Разработка кастомных алгоритмов маскирования
- Маскирование BigData как в режиме Update, так и в режиме Insert
- Разработка системы автоматизации (встраивание в цикл безопасной разработки ПО)
- Маскирование сложных коробочных решений







SecretTechnologies

Спасибо за внимание!

Москва, Волгоградский пр-т,
дом 43, корпус 3, офис 723,
БЦ «Авилон Плаза»

☎ +7 (495) 109-29-50
✉ sales@secretgroup.ru
🌐 www.secretgroup.ru