**ОПРОС: БЕЗОПАСНОСТЬ ДАННЫХ В DATA ENGINEERING**

**БЛОК A: ДЕМОГРАФИЯ И КОНТЕКСТ**

**1. Ваша основная роль (единичный выбор)**

* Data Engineer
* Data Scientist
* Analytics Engineer
* ML Engineer
* Data Analyst
* DevOps Engineer
* Security Engineer
* Team Lead/Manager
* Другое: \_\_\_\_\_\_

**2. Опыт работы в сфере данных (единичный выбор)**

* Менее 1 года
* 1-3 года
* 3-5 лет
* Более 5 лет

**3. Размер компании (единичный выбор)**

* Стартап (1-50 сотрудников)
* Малая компания (51-200)
* Средняя компания (201-1000)
* Крупная компания (1000+)

**4. Отрасль компании (единичный выбор)**

* FinTech/Банкинг
* E-commerce/Retail
* Здравоохранение
* Телеком
* SaaS/Технологии
* Госсектор
* Образование
* Другое: \_\_\_\_\_\_

**БЛОК B: ТЕКУЩЕЕ СОСТОЯНИЕ БЕЗОПАСНОСТИ**

**5. Как вы оцените общий уровень безопасности данных в вашей компании? (единичный выбор)**

* Очень высокий
* Высокий
* Средний
* Низкий
* Очень низкий

**6. Какие данные вы обрабатываете? (множественный выбор)**

* Персональные данные (PII)
* Финансовые данные
* Медицинские данные
* Коммерческая тайна
* Публичные данные
* Логи и метрики
* Другое: \_\_\_\_\_\_

**7. Соответствуете ли вы регуляторным требованиям? (единичный выбор)**

* GDPR
* CCPA
* HIPAA
* SOX
* PCI DSS
* Не соответствуем
* Не знаю

**БЛОК C: ИНСТРУМЕНТЫ И ПРАКТИКИ**

**8. Какие инструменты безопасности используете? (множественный выбор)**

* Шифрование данных (at-rest)
* Шифрование данных (in-transit)
* Masking/Tokenization данных
* Системы управления доступом (RBAC)
* Мониторинг и аудит доступа
* DLP-системы
* SIEM-системы
* Сканеры уязвимостей
* Не используем специальные инструменты

**9. Как реализовано управление доступом? (единичный выбор)**

* RBAC с детальными правами
* Базовое управление доступом
* Доступ по принципу "need-to-know"
* Свободный доступ внутри команды
* Не структурировано

**10. Частота проведения аудитов безопасности (единичный выбор)**

* Ежеквартально или чаще
* Полугодово
* Ежегодно
* По требованию
* Никогда

**БЛОК D: РИСКИ И ИНЦИДЕНТЫ**

**11. Сталкивались ли с инцидентами безопасности за последний год? (единичный выбор)**

* Да, несколько раз
* Да, один раз
* Нет
* Не знаю/не уверен

**12. Какие основные риски безопасности беспокоят? (множественный выбор)**

* Утечки данных
* Неавторизованный доступ
* Внутренние угрозы
* Внешние атаки
* Ошибки конфигурации
* Несоблюдение compliance
* Потеря данных

**13. Время обнаружения инцидента (единичный выбор)**

* Менее 1 часа
* 1-24 часа
* 1-7 дней
* Более 7 дней
* Не измеряем

**БЛОК E: КУЛЬТУРА И БУДУЩЕЕ**

**14. Как часто проходит обучение безопасности? (единичный выбор)**

* Ежеквартально
* Полугодово
* Ежегодно
* При приеме на работу
* Никогда

**15. Бюджет на безопасность данных (единичный выбор)**

* Значительно увеличился
* Умеренно увеличился
* Не изменился
* Сократился
* Не знаю

**16. Планы по улучшению безопасности (множественный выбор)**

* Внедрение новых инструментов
* Усиление мониторинга
* Обучение команды
* Автоматизация compliance
* Пересмотр процессов
* Нет планов