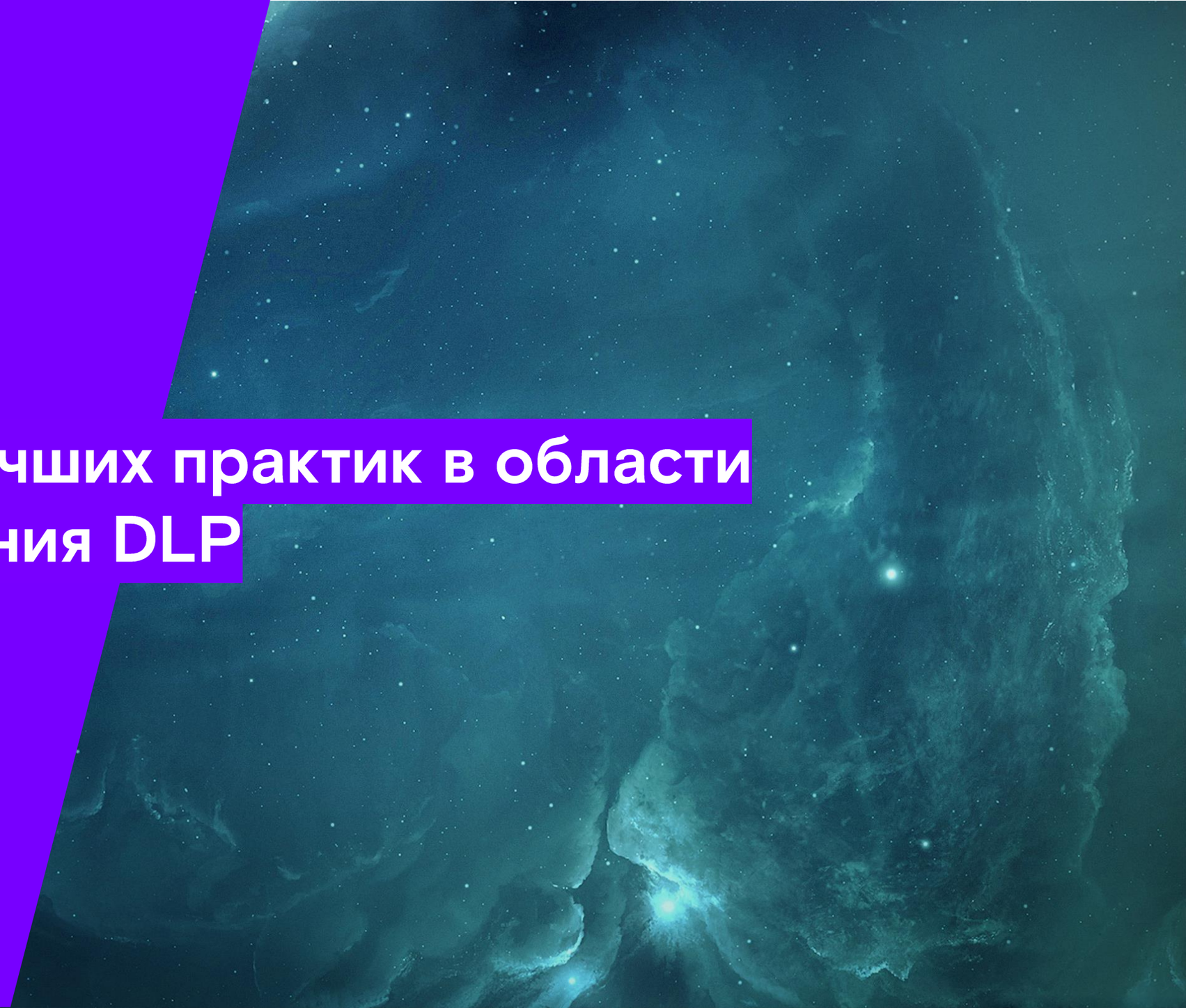
Ростелеком
Солар

ТОП 5 лучших практик в области применения DLP



Спикер

Контакты:

+7 905 755 66 22

s.hudyakova@rt-solar.ru

Софья Худякова

Руководитель отдела продуктовой аналитики «Ростелеком-Солар»

Опыт и экспертиза

- Разработка продуктов в области информационной, экономической и кадровой безопасности
- Автоматизация предприятия
- Системная интеграция
- Автоматизация бизнес-процессов
- Бизнес-анализ
- Системный анализ
- Управление проектами
- Системное мышление

Ростелеком Солар

1200 новых уведомлений

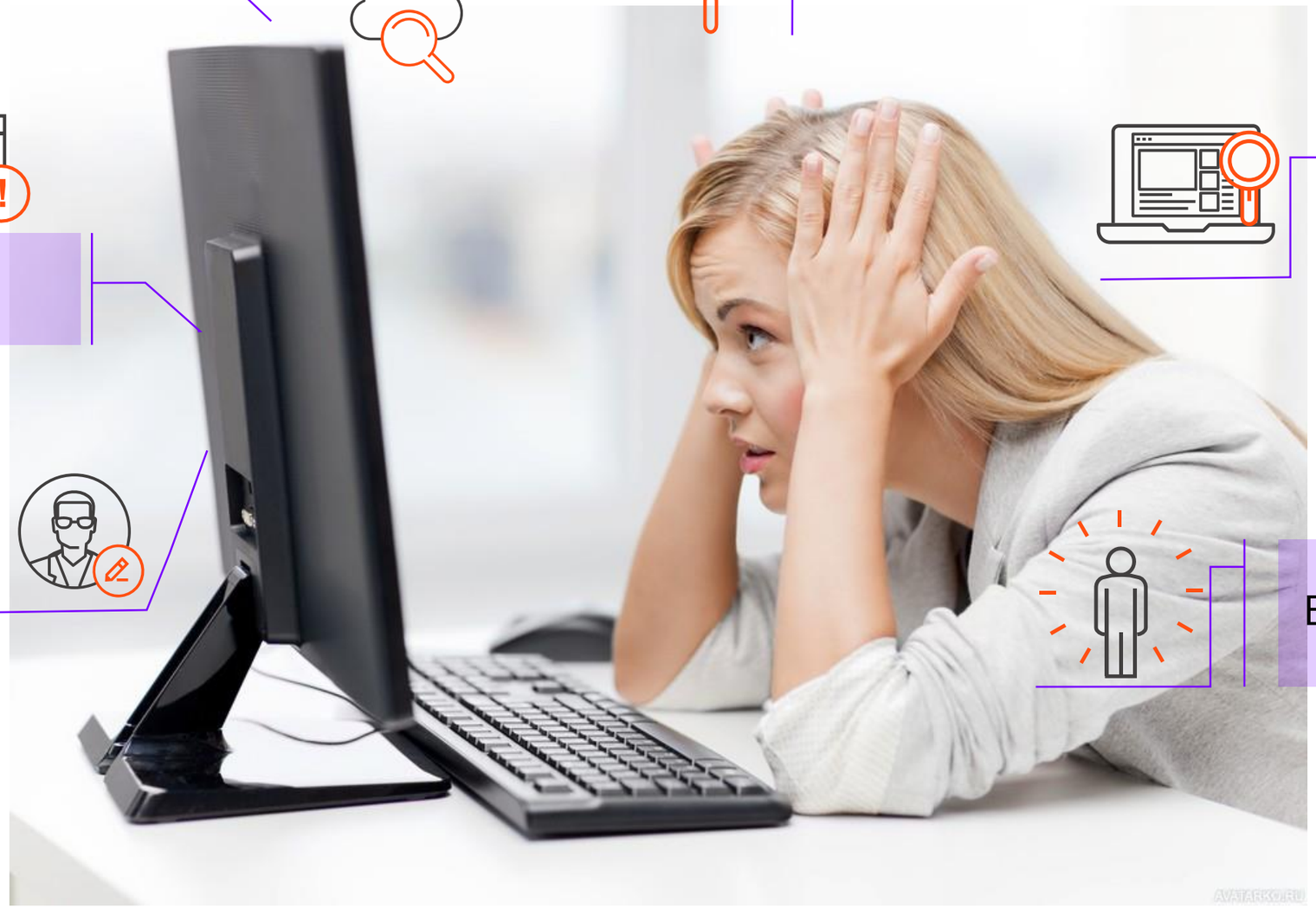
Расследовать новый инцидент

Alert!

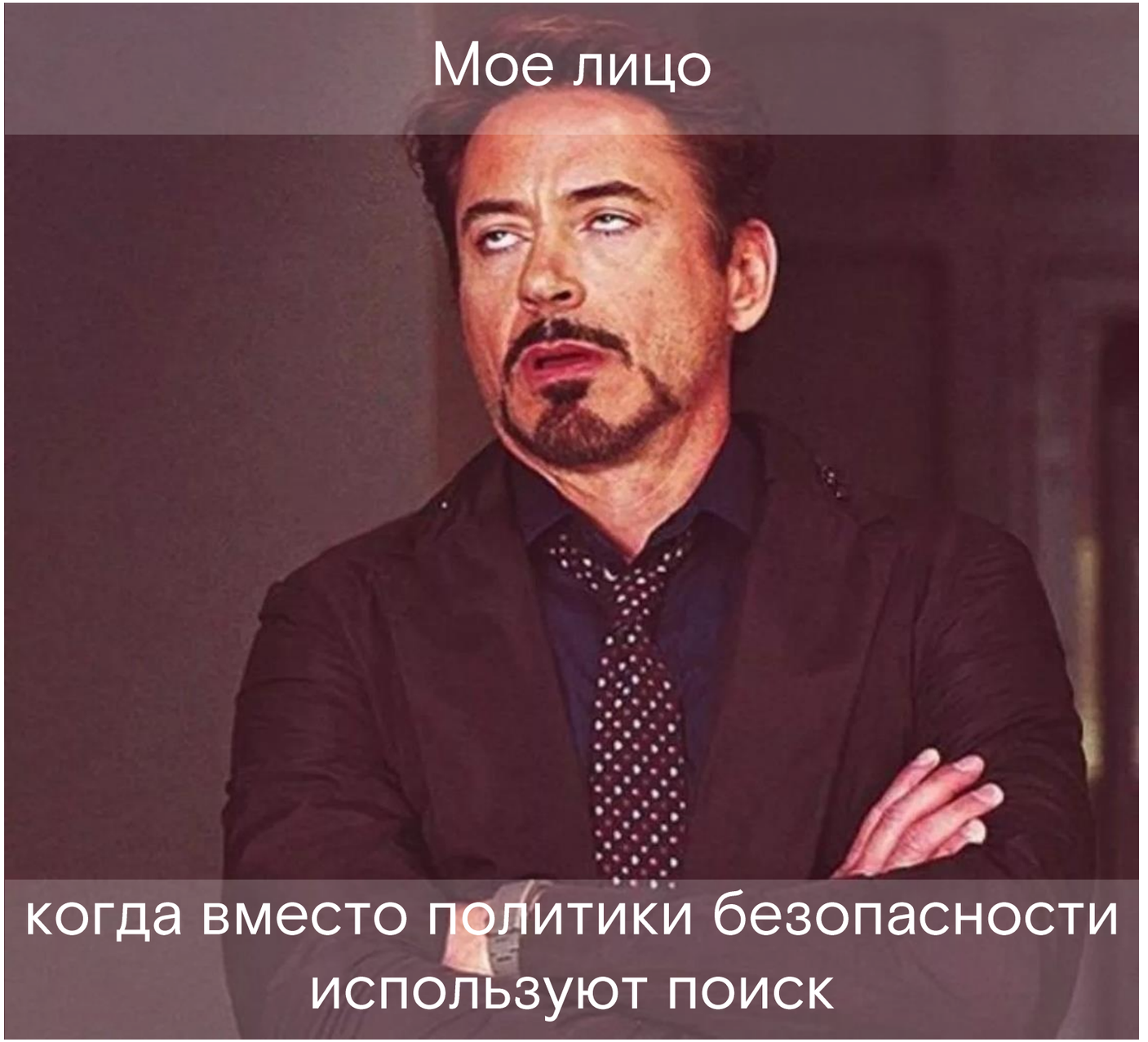
Предоставить отчет

Нарушитель

Взять на контроль



Ростелеком Солар



Ростелеком
Солар

Политика безопасности vs Поиск

Поиск

- Простой и понятный механизм
- Создает иллюзию контроля
- Не исключает человеческий фактор
- Обработка результатов отнимает много времени

Политика безопасности

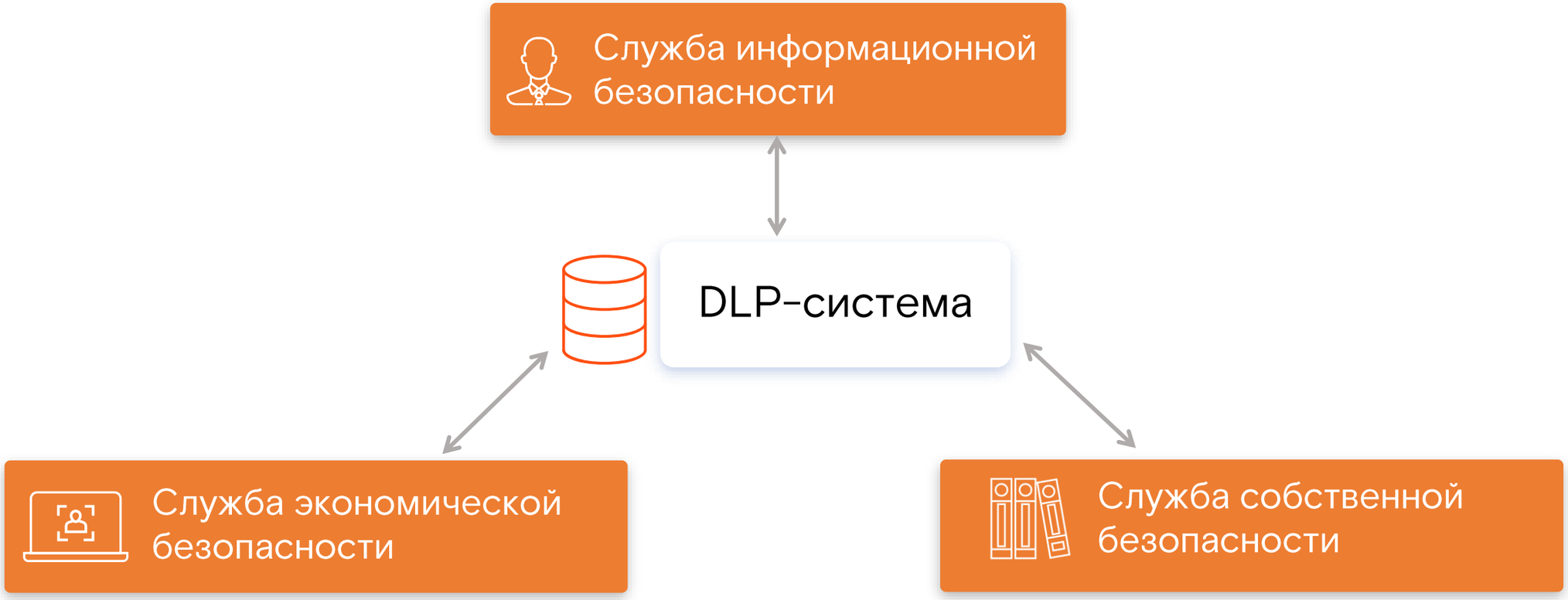
- Избавит от человеческой ошибки
- Найдет скрытую утечку
- Автоматически создаст инцидент
- Отправит уведомление офицеру ИБ

Практика: используйте политику DLP-системы, а не поиск

Ростелеком Солар

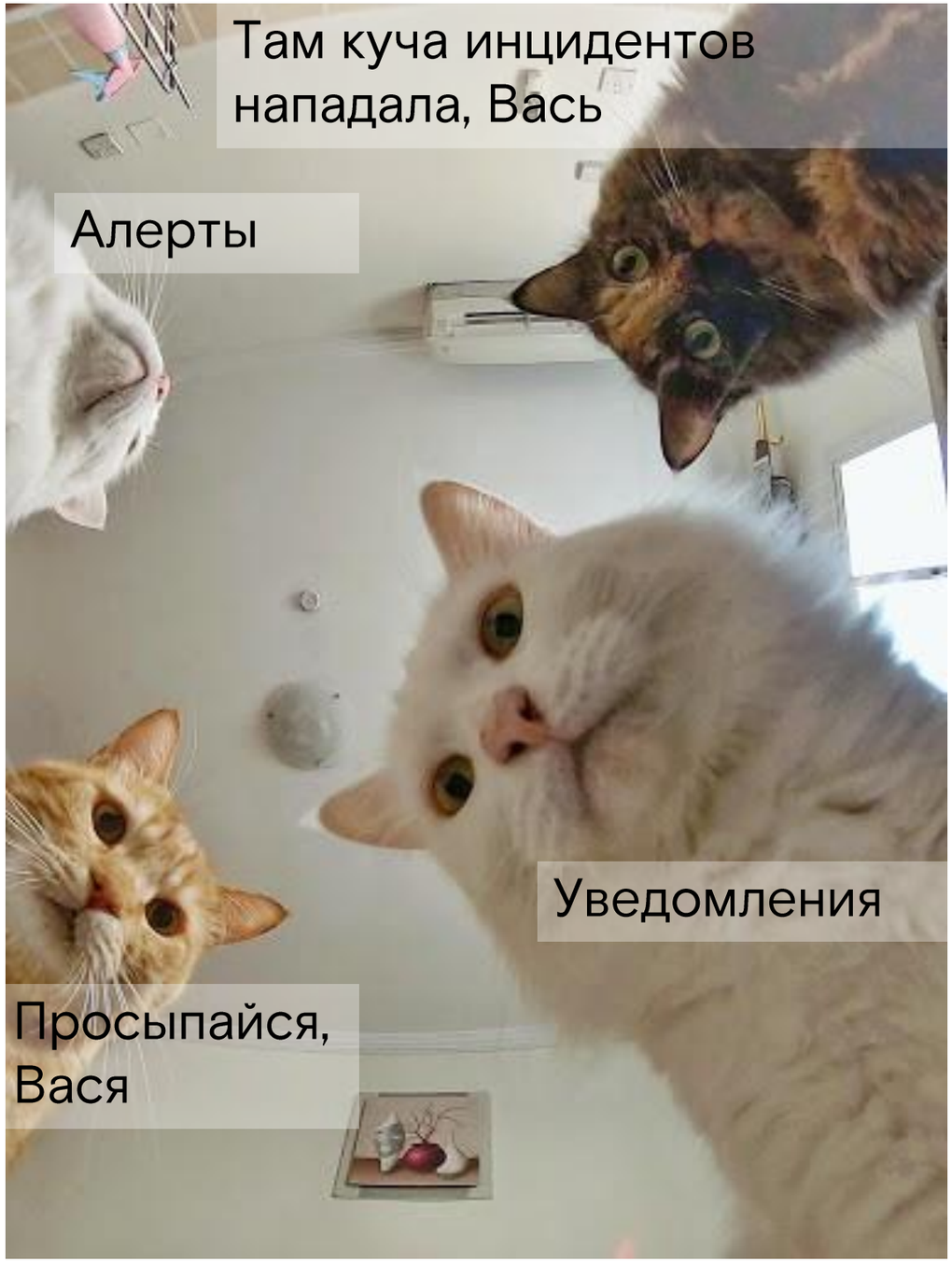
Ростелеком
Солар

Совместная работа в DLP: ролевая модель



Практика: организуйте совместный доступ

Ростелеком Солар



Ростелеком
Солар

Генеральная уборка: отсекаем лишнее

Ненужные политики:

- засоряют и нагружают систему
- задерживают обработку событий
- могут вызвать технические проблемы

Практика: удаляйте ненужные, лишние политики

Ростелеком Солар

Жизнь после внедрения DLP:

Ожидание

Реальность

Ростелеком
Солар

Тюнинг DLP-политик

Шаг 1 - исключаем утечки

- Утечка – реальный риск для организации
- Требует немедленного пересмотра политики

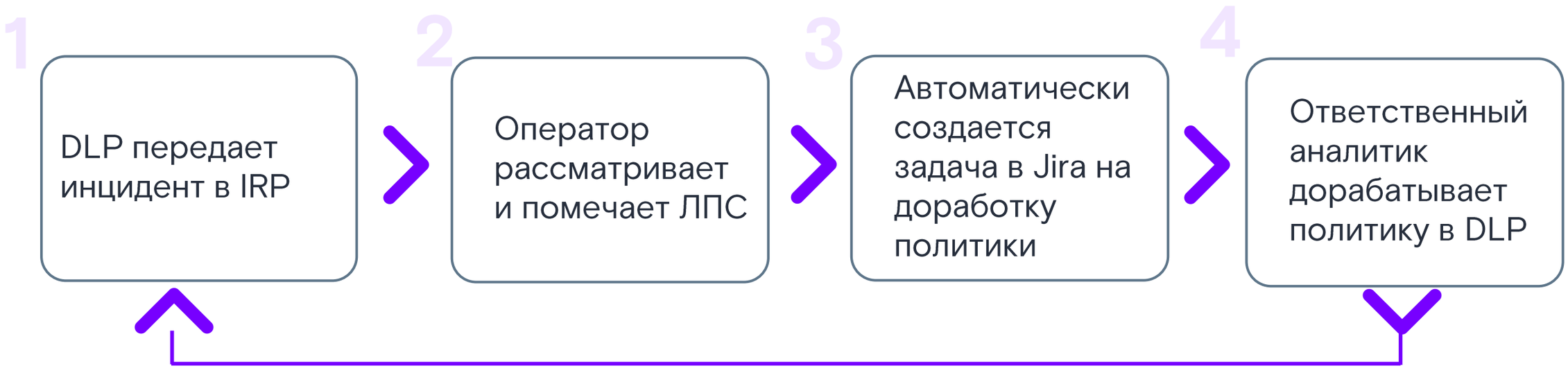
Шаг 2 – минимизируем ЛПС

- Засоряет пул событий
- Затрудняет поиск реальных инцидентов
- Требует настройки исключений

Тюнинг политики - это непрерывный процесс

Ростелеком Солар

Как можно автоматизировать процесс тюнинга политик

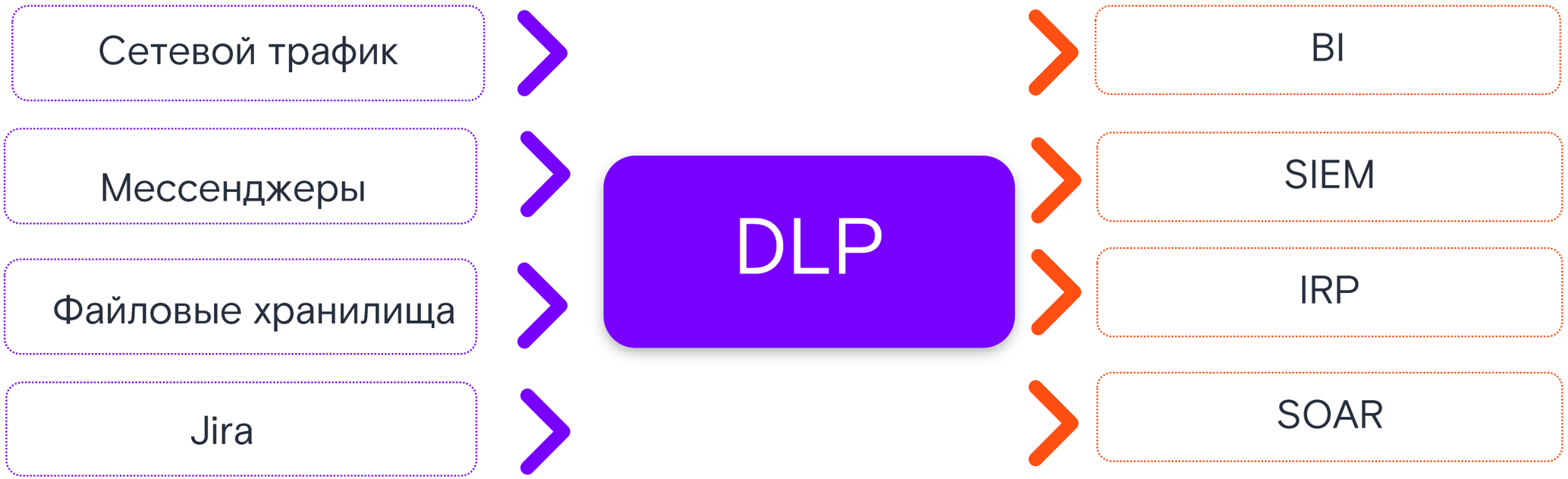


Тюнинг политики – это непрерывный процесс

Ростелеком Солар

Ростелеком
Солар

Интеграция DLP-систем со стеком ИТ/ИБ- и бизнес-решений



Практика: расширяйте использование DLP-систем

Ростелеком Солар

Чек-лист практик применения DLP

1. Пользуйтесь политикой DLP-системы (а не поиском)
2. Организуйте совместный доступ (ролевая модель)
3. Удаляйте ненужные, лишние правила политики
4. Сделайте доработку политик своей рабочей рутиной
5. Расширяйте использование DLP-системы (интеграции)

Ростелеком
Солар

Спасибо!

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

solar@rt-solar.ru

+7 905 755 66 22

s.hudyakova@rt-solar.ru