БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

DLP как источник данных для работы системы выявления внутреннего мошенничества

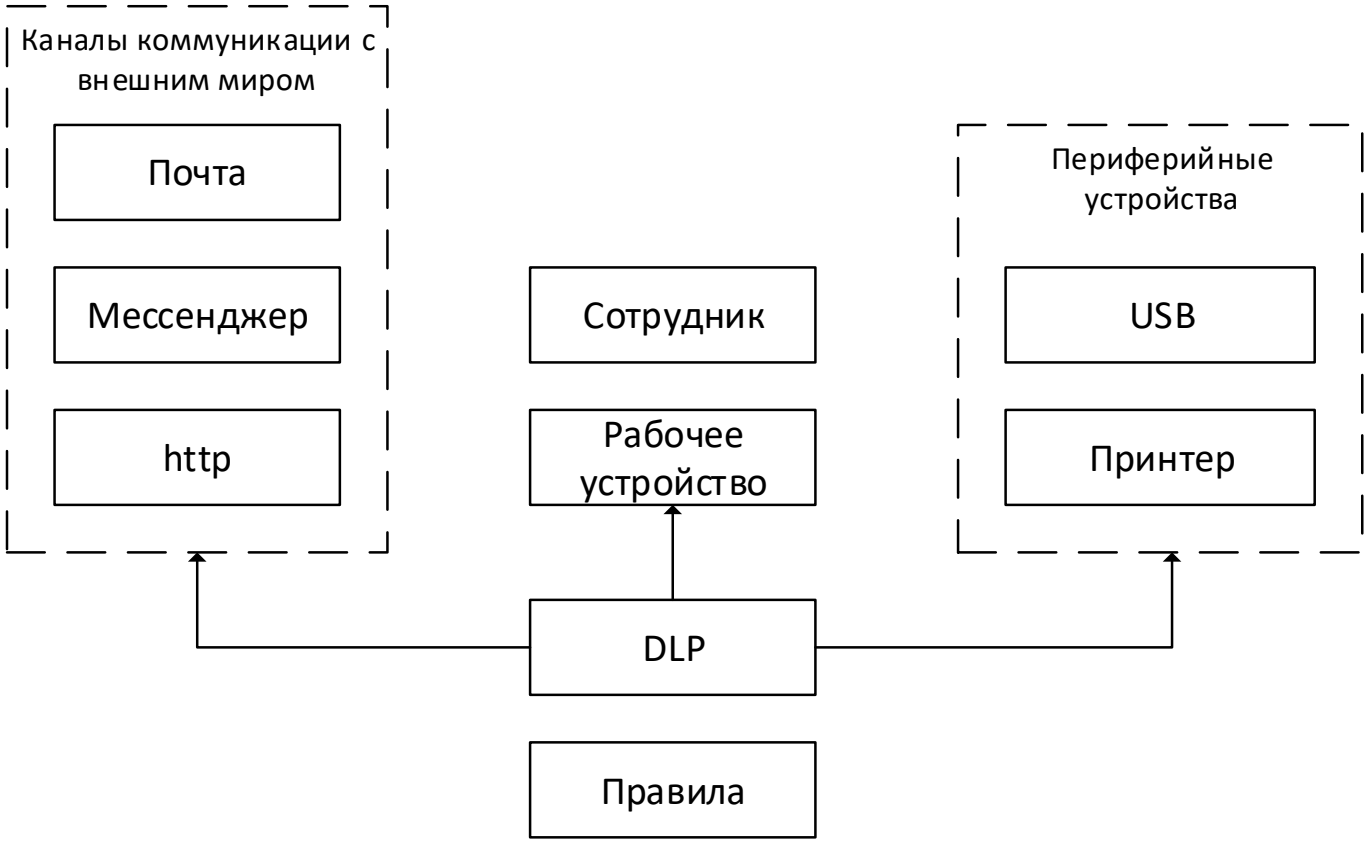
Зачем?

Снижение рисков:

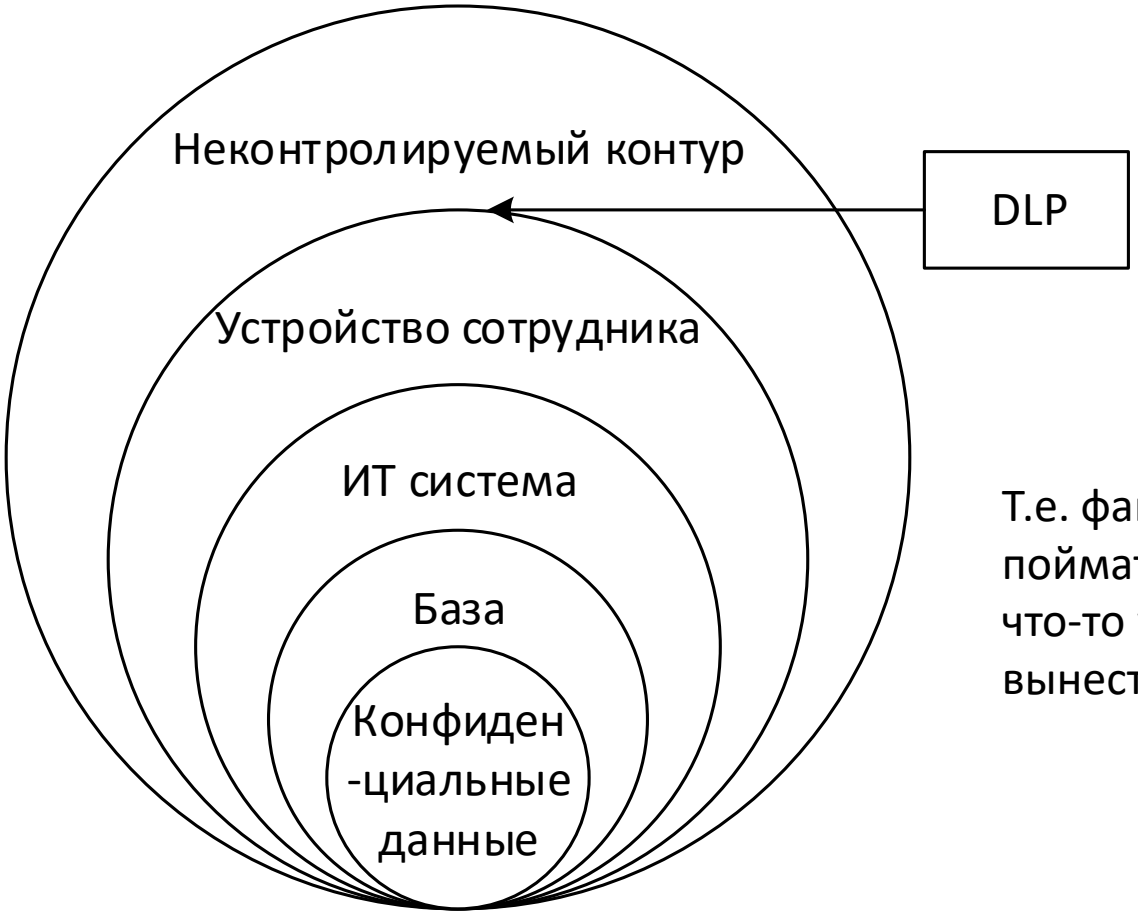
1. Внесение несанкционированных изменений
2. Разглашение конфиденциальных данных

Какие задачи решает DLP?

Защита от утечки данных.
А достаточно ли DLP для защиты от разглашения конфиденциальных данных?



Какие задачи решает DLP?



Т.е. фактически, DLP пытается поймать человека, который уже что-то украл и пытается вынести.

Чего не хватает DLP?

№	Недостаток	Последствия
1	В DLP фактически отсутствует информация о работе сотрудника с конфиденциальной информацией в корпоративных системах.	Нет возможности выявить признаки утечки данных на ранних стадиях
2	DLP не учитывает инциденты, связанные с сотрудником, вывяленные SOC	Как правило, для построения профиля сотрудника, DLP использует собственные данные по инцидентам
3	DLP не учитывает попытки нарушения сотрудником установленных правил доступа.	Как правило, нарушитель в какой-то момент начинает исследовать доступные системы на возможность выгрузки конфиденциальных данных
4	DLP не выявляет аномалии в работе сотрудника с корпоративными ИТ системами	

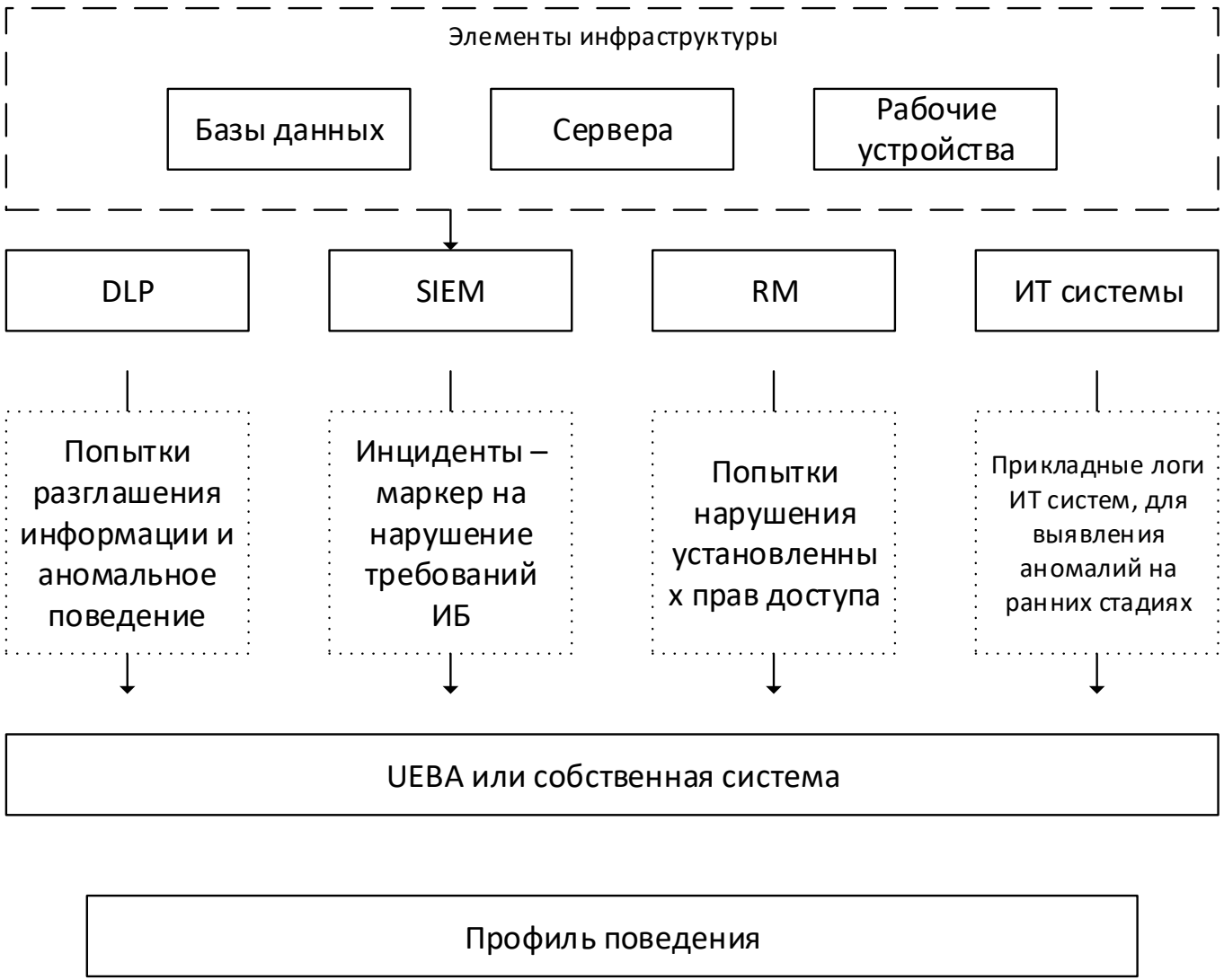
Спасет ли UEBA?

Да, но …

1. Готовые системы очень дороги.

2. Готовые системы также требуют настройки

Вариант системы



Выводы

1. Аномальное поведение необходимо выявлять на максимально ранних стадиях.
2. DLP является хорошим инструментом, позволяющим выявить попытки разглашения данных, которые уже были выгружены.
3. Система управления правами должна соответствовать актуальному перечню ИТ система для обеспечения возможности автоматизированного контроля.
4. Сценарии SOC должны обеспечивать контроль за нарушением существующих требований ИБ. Это позволит выявить опасное поведение сотрудников на ранних стадиях.
5. Доступ к конфиденциальным данным должен быть строго персонифицированным.
6. Необходимо минимизировать каналы прямого взаимодействия устройства сотрудника с публичными системами и сервисами. Если на рабочем устройстве установлен мессенджер и есть возможность сохранять данные в гугл драйв, то вероятность разглашения конфиденциальных данных существенно повышается

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Беляков И.А.
bia@bspb.ru

Спасибо за внимание!