



## DLP как сервис

Руководитель направления по DLP-системам  
Микулин Борис

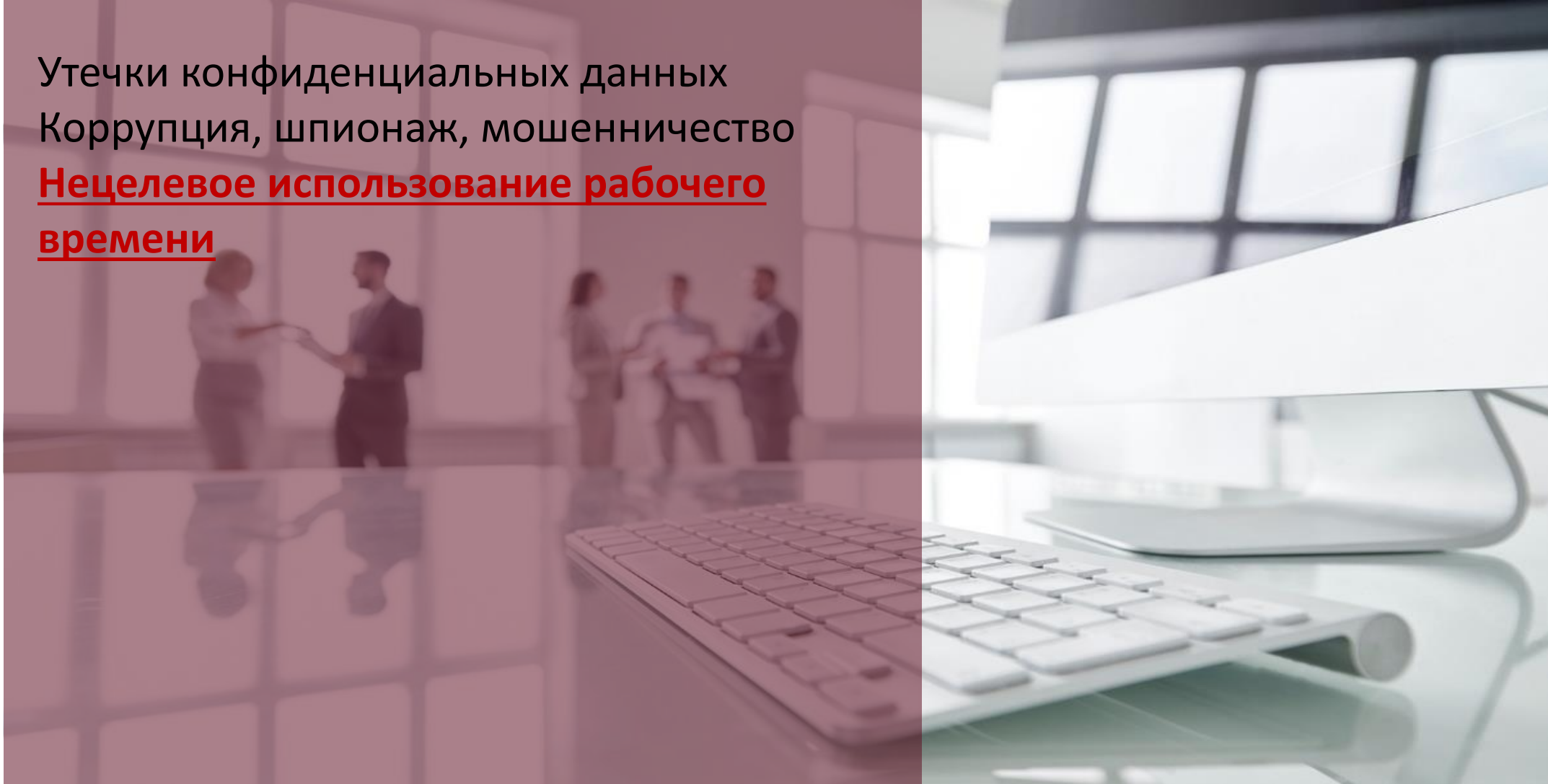
Дата: 26.03.2019

# Особенности компании

- Большие объемы информации
- Множество систем по ИБ
- Нехватка человеческих ресурсов
- Сложная структура документооборота

# Риски

Утечки конфиденциальных данных  
Коррупция, шпионаж, мошенничество  
**Нецелевое использование рабочего времени**



# Кому поможет DLP-система



## Собственники бизнеса, ТОП-менеджмент

- предотвращение ущерба / возврат потерь
- исполнение требований законов
- формирование доказательной базы
- обнаружение уязвимостей в бизнес-процессах



## ИБ

- предотвращение утечек КИ
- контроль движения КИ
- дополнительные сведения по инцидентам



## СБ

- контроль взаимодействия с партнёрами
- сбор информации о бизнес-процессах
- поиск инсайдеров
- контроль неформальных связей в организации и нетипичных контактов
- защита наиболее критичных процессов и ценных кадров



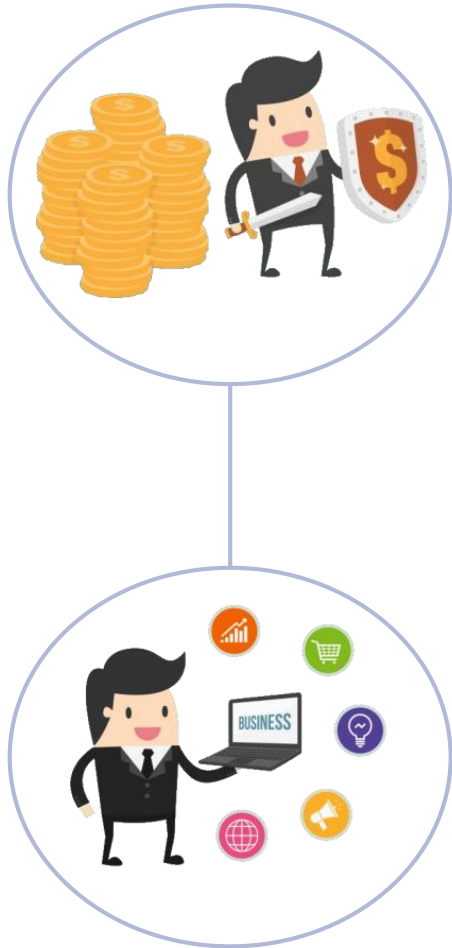
## Функциональные руководители / HR

- эффективность сотрудников
- обстановка в коллективе
- уязвимость и лояльность сотрудников

# Проблематика (Предпосылки к передаче DLP на аутсорсинг)

- Отсутствие людских ресурсов / компетенций у заказчика для ее сопровождения
- Большое количество событий системы DLP
- Проблемы с настройкой системы DLP
- Отсутствие процессов выявления фактов утечки информации и реагирования на инциденты, связанные с утечкой информации
- Желание использовать все возможности DLP, но страх перед необходимостью погружаться в технические процессы
- Нежелание / сложности найма и обучения персонала под задачи DLP

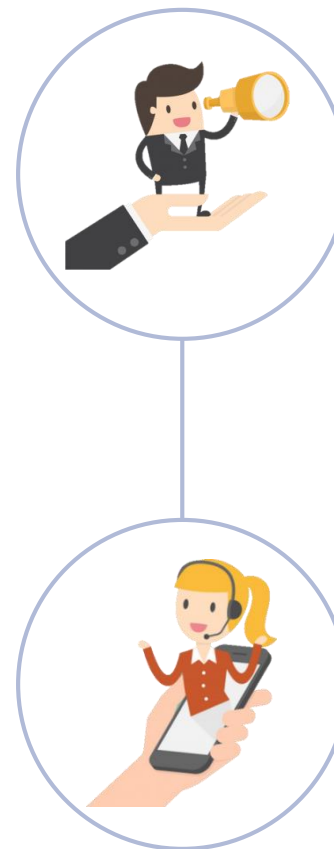
# Аутсорсинг возможностей DLP



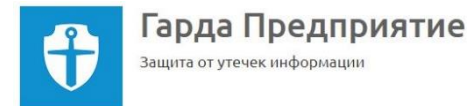
- Контроль всех потоков информации, пересекающих периметр
- Выявление фактов хранения и передачи конфиденциальной информации вне бизнес-процессов
- Проверка соблюдения регламентов и процедур
- Разоблачение мошеннических схем
- Расследование инцидентов

## Как это работает

- Передача всех работ высококлассным специалистам
- Работа с системой в режиме полного рабочего дня
- Оперативное предоставление информации и отчетов
- Отсутствие необходимости со стороны Заказчика погружаться в технические подробности системы



# Вендоры





# Сервисы

Мониторинг каналов

Расследования

Профилирование

## Сервисы

### Мониторинг каналов

- Точечно настраиваем политики DLP
- Выявляем утечки (с возможностью предоставления отчета)
- Отсеиваем ложные
- Пишем сопроводительную записку
- Дополняем полезной информацией (какие документы нарушены, первое ли нарушение, скорое увольнение сотрудника)
- Направляем Заказчику

Расследования

Профилирование

# Сервис. Мониторинг каналов. Как это работает?



# Сервисы

Мониторинг каналов

## Расследования

- Получение запроса на поиск информации по определенной теме (**НЕ ТОЛЬКО ИНЦИДЕНТЫ ИБ**)
- Анализ архива DLP и доп. информации
- Предоставление подробного отчета и сопутствующих материалов (копии документов, логи действий и т.п.)

Профилирование

# Сервисы

Мониторинг каналов

Расследования

Профилерование

- Анализ эффективности работы сотрудников (чем занимается на работе)
- Определение их лояльности к компании (есть ли негатив к руководству/коллегам)
- Выявление «групп риска» среди сотрудников (долги, наркотики, азартные игры...)

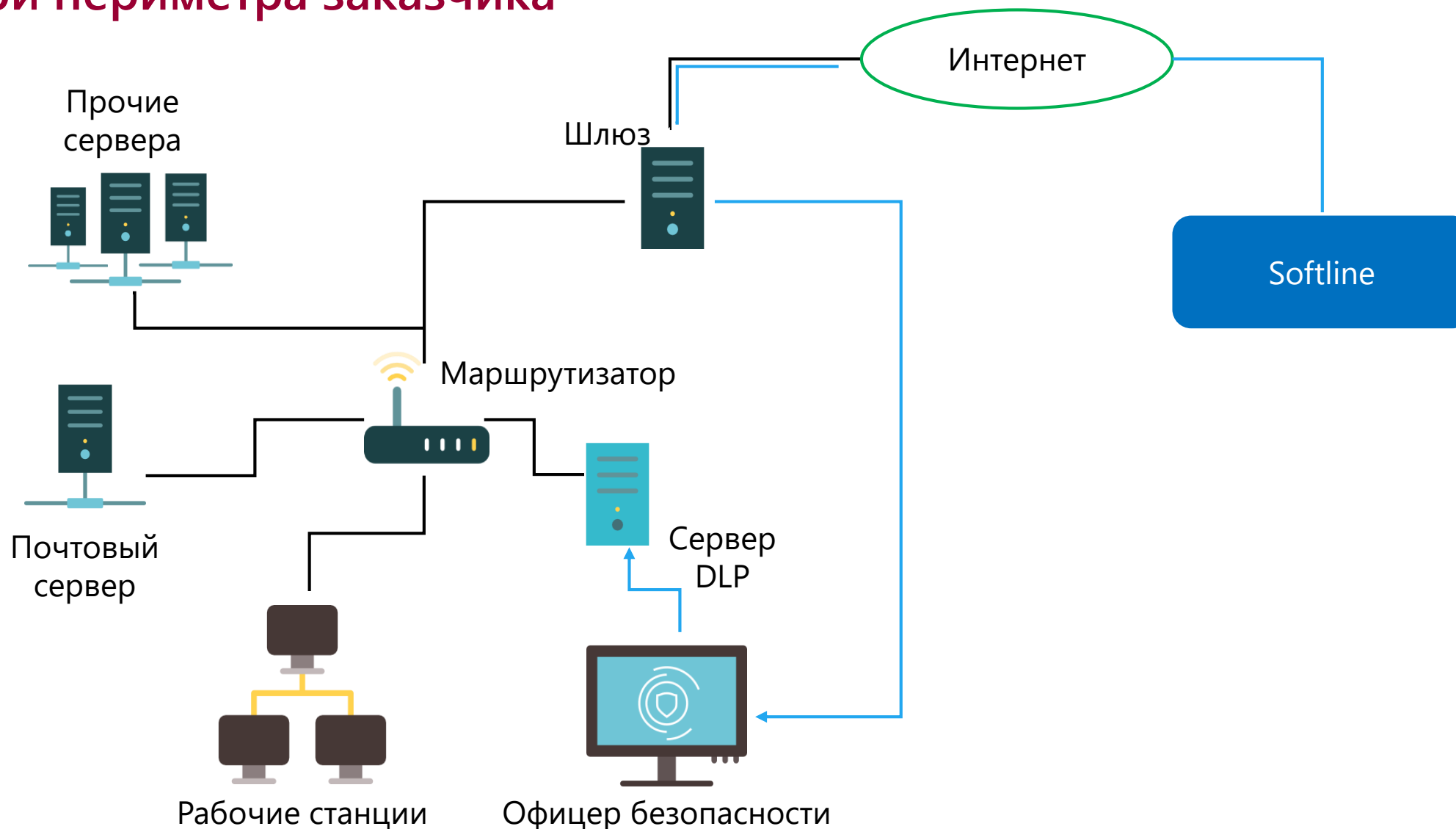
# Сервис. Профилирование. Как это работает?



A low-angle, upward-looking photograph of several modern skyscrapers with glass facades. The buildings are set against a bright blue sky with scattered white clouds. The perspective creates a sense of height and scale. A prominent red rectangular box is overlaid on the left side of the image, containing the word 'Реализация' in white text.

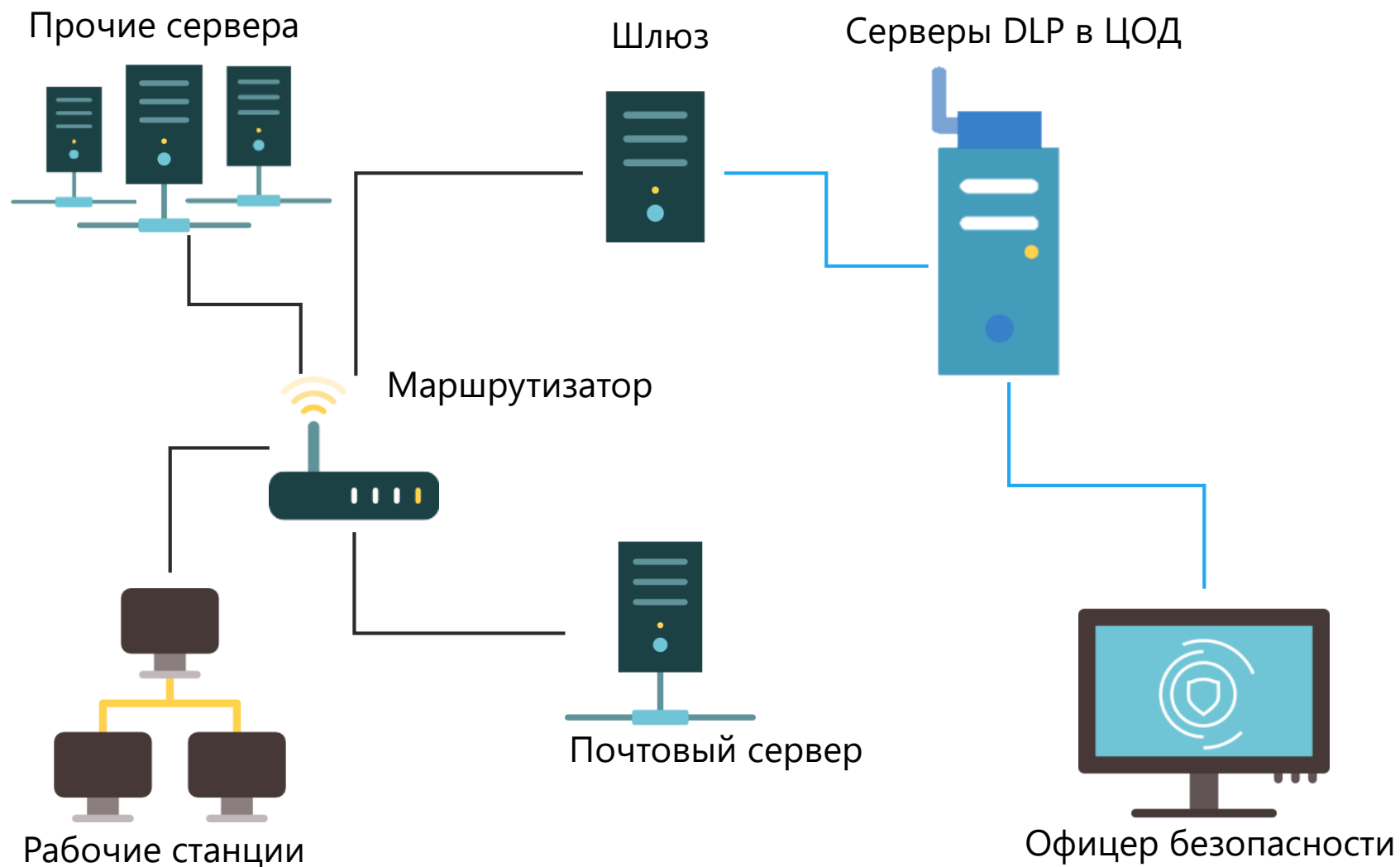
Реализация

# Внутри периметра заказчика





## За периметром (облака)



# Плюсы заказчика

Избавляем от:

- Необходимости вникать в технические процессы
- Проблем с выбором решения и его закупкой
- Внедрения и дальнейшего сопровождения работы системы DLP
- Сложностей коммуникаций с вендорами на всех этапах
- Необходимости поиска и обучения собственных аналитиков и инженеров
- Переключения на работу с DLP уже занятых другими задачами сотрудников
- Самостоятельного построения процессов реагирования на инциденты, связанных с утечкой данных

# Состав и стоимость работ

СЕРВИС	СТОИМОСТЬ НА 1000 АРМ
<b>МОНИТОРИНГ КАНАЛОВ УТЕЧКИ</b> Контроль обработки, передачи и хранения конфиденциальной информации	от 1 млн рублей / год
<b>РАССЛЕДОВАНИЯ</b> Поиск информации по интересующей тематике, анализ и составление отчета	от 1 млн рублей / год
<b>ПРОФИЛИРОВАНИЕ</b> Мониторинг активности пользователей, формирование рискованных групп, точечный контроль за персоналом из этих групп	от 2 млн рублей / год

# Обоснование для заказчика

ЗАКАЗЧИК	СЕРВИС DLP
<ul style="list-style-type: none"><li>• Сложности с поиском специалистов узкой направленности, их дальнейшее развитие, риск ухода</li><li>• В случае временного отсутствия сотрудника, ответственного за работу с DLP, высок риск пропустить инцидент</li><li>• Работа с системой может быть только из задач сотрудника, из-за чего ей будет уделяться меньше времени, как следствие, система будет работать не на 100 %</li></ul>	<ul style="list-style-type: none"><li>• Передача всех работ высококлассным специалистам с непредвзятым отношением к сотрудникам компании (исключение сговора)</li><li>• Работа с системой в режиме полного рабочего дня, соблюдение SLA</li><li>• Оперативное предоставление информации и отчетов</li><li>• Отсутствие необходимости со стороны Заказчика детально погружаться в работу системы</li><li>• Прозрачные расходы на сервис, упрощение обоснования затрат</li></ul>
<p>ФОТ: 1 аналитик ≈ 120 тыс. руб / месяц Отчисления/ обязательные выплаты ≈ 40 тыс. руб / месяц</p> <p><b>1.92 млн. руб в год</b></p>	<p>Цена:</p> <p><b>От 1 млн. руб в год</b> с возможностью выбрать необходимые опции и варьировать стоимость</p>



Спасибо за внимание.

Руководитель направления по DLP-системам

Микулин Борис

[Boris.Mikulin@softlinegroup.com](mailto:Boris.Mikulin@softlinegroup.com)

8-9999-71-63-06

Дата: 26.03.2019