



DLP: АНАЛИТИЧЕСКОЕ
СОПРОВОЖДЕНИЕ

Александр Дворянский

КОМУ НУЖНА DLP-СИСТЕМА

DLP (Data Loss Prevention) – система для предотвращения утечек конфиденциальной информации, проведения расследований и мониторинга сотрудников.

Владельцам и топ-менеджменту

Избежать финансовых и репутационных потерь

Обеспечить соответствие законодательным требованиям

Службе ИБ

Предотвращать утечки конфиденциальной информации

Получать дополнительные сведения по инцидентам

Службе безопасности

Контролировать взаимодействие с партнерами

Отслеживать неформальные связи и нетипичные контакты в организации

Руководителям и HR

Оценивать эффективность и лояльность сотрудников

Анализировать обстановку в коллективе

ПРЕДПОСЫЛКИ К ПЕРЕДАЧЕ DLP НА АУТСОРСИНГ

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

НАШИ СЕРВИСЫ

Первичная консультация

Внедрение DLP

Пилот DLP

Обучение

Подбор и поставка DLP-решения

Техподдержка и аналитика



АНАЛИТИЧЕСКОЕ СОПРОВОЖДЕНИЕ



МОНИТОРИНГ КАНАЛОВ

Контроль обработки,
передачи и хранения
конфиденциальной информации



РАССЛЕДОВАНИЯ

Поиск информации по запросу,
анализ и составление отчета



ПРОФИЛИРОВАНИЕ

Контроль эффективности
и лояльности сотрудников
компании

ПРИМЕР ПРОЕКТА: ФИНАНСОВАЯ КОМПАНИЯ

ИСХОДНЫЕ ДАННЫЕ:

30 000 сотрудников

> 10 филиалов по всей стране

5 лет срок хранения данных

ВЫБРАННЫЕ СЕРВИСЫ:

Мониторинг каналов, расследования, профилирование

РЕЗУЛЬТАТ В СРЕДНЕМ ЗА ГОД:

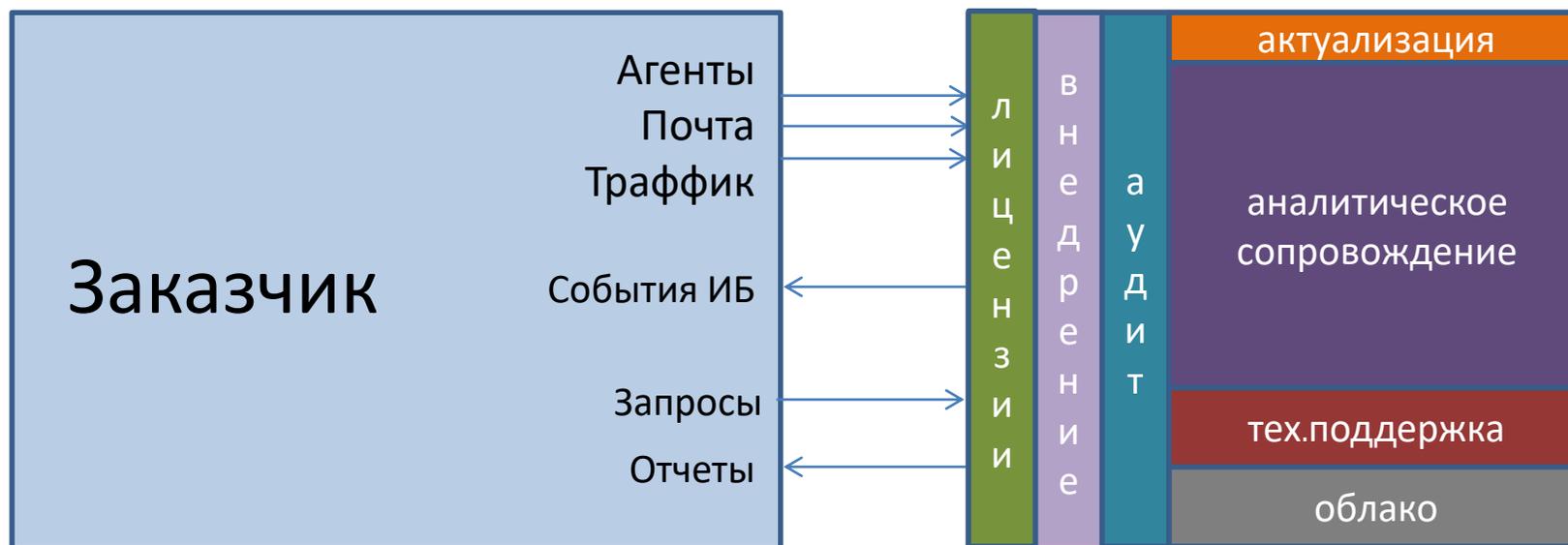
3000 инцидентов на обработку

300 запросов на расследования

200 человек на ежедневном особом контроле

5 служебных расследований переданы в МВД

ПРИНЦИП РАБОТЫ

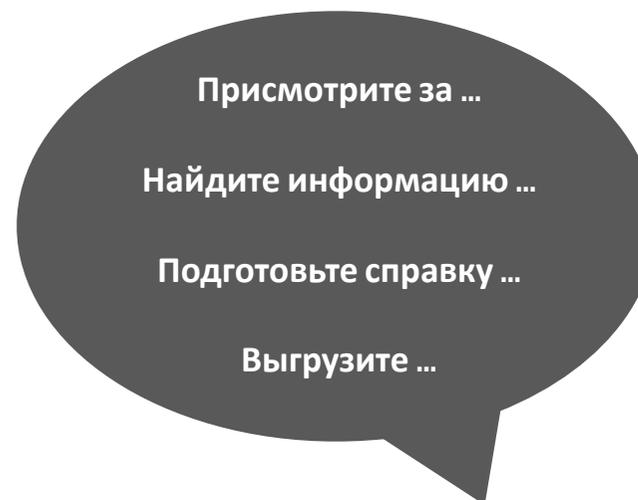


КАК ЭТО РАБОТАЕТ

Серверы DLP



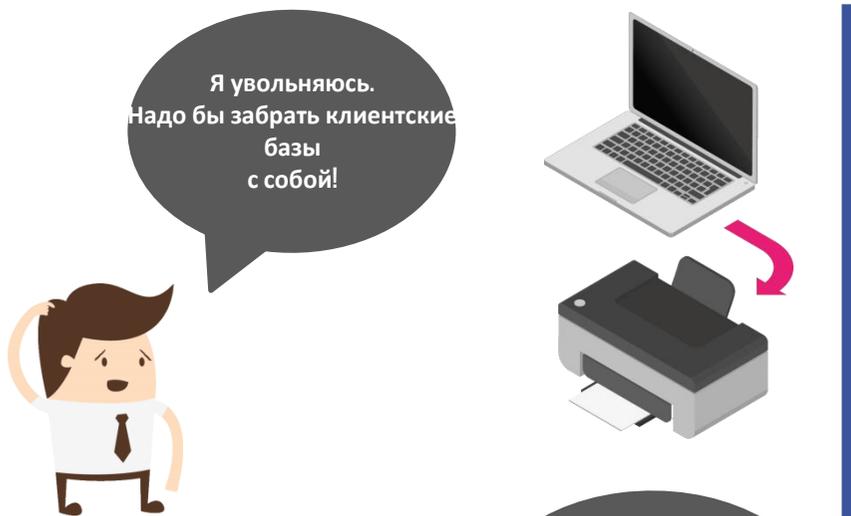
Аналитики
Инфосекьюрити



Заказчик

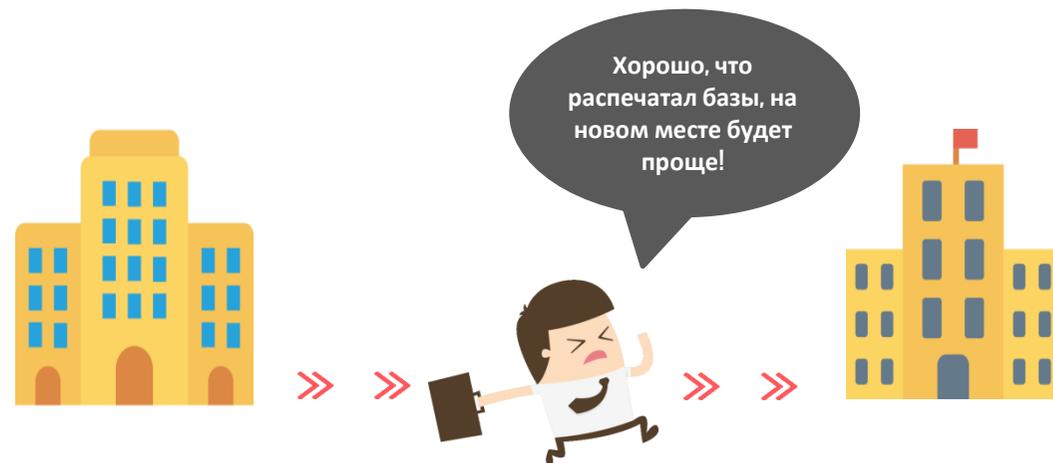


МОНИТОРИНГ КАНАЛОВ



Я увольняюсь. Надо бы забрать клиентские базы с собой!

Illustration of a man in a white shirt and tie standing next to a laptop and a printer. A pink arrow points from the laptop to the printer.



Хорошо, что распечатал базы, на новом месте будет проще!

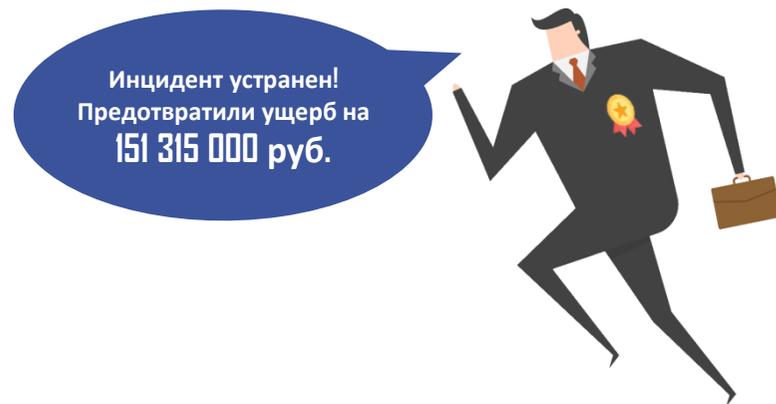
Illustration of a man in a white shirt and tie running with a briefcase between two yellow buildings. Red double arrows indicate movement.



Он распечатал базу!

Мы знаем, что ты распечатал базу! Событие перехвачено Инфосекьюрити!

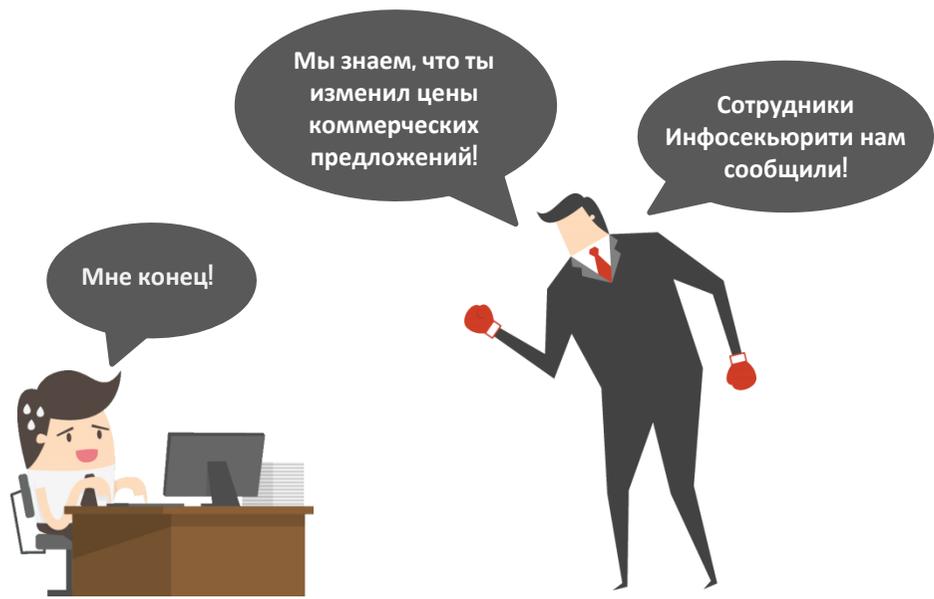
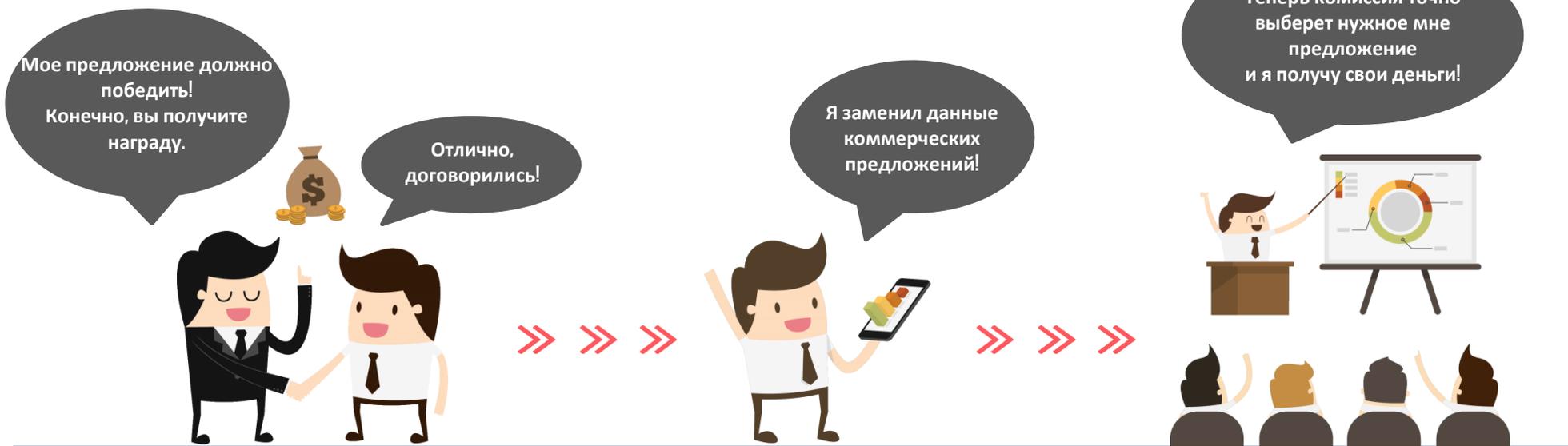
Illustration of a woman in a black suit standing by a yellow building. A man in a white shirt and tie is being confronted by a man in a black suit and red boxing gloves. Red double arrows indicate movement.



Инцидент устранен! Предотвратили ущерб на 151 315 000 руб.

Illustration of a man in a black suit and red boxing gloves running with a briefcase and a gold medal on his chest. A blue speech bubble contains the text.

РАССЛЕДОВАНИЯ



ПРОФИЛИРОВАНИЕ

Ого! Хорошее предложение от компании-конкурента!

Уволюсь и устроюсь к ним! И, конечно, заберу свою команду инвесторов!

Я уйду! Здесь все плохо, а там хорошо! Пойдемте со мной!

Сотрудник увольняется!

Он хочет забрать инвесторов с собой!

INFO SECURITY

Надо срочно уладить конфликт и изолировать сотрудника от коллектива!

Все хорошо!

Работаем дальше!

Предотвратили ущерб на 786 000 000 руб.

INFO SECURITY

МИФЫ И ЗАБЛУЖДЕНИЯ

Мы становимся вашими заложниками

Настройте ограничение доступа. За плечами «Инфосекьюрити» 8 лет безупречной работы. Все наши сотрудники проходят регулярные проверки на полиграфе.

Все это слишком дорого

Ущерб от инцидента может быть намного больше. Вы не тратитесь на поиск и обучение своих аналитиков. Для оптимизации цены у нас есть гибкий калькулятор.

Зачем нам тогда СБ и ИБ?

Мы дополняем, а не заменяем. Совместная работа более эффективна. При этом СБ и ИБ могут освободить ресурсы под другие важные задачи.

Наша DLP вам не подойдет?

Мы работаем со всеми DLP-системами, знаем их сильные и слабые стороны. Можем использовать вашу систему или предложить лучший вариант.

ОБОСНОВАНИЕ

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

ПЛЮСЫ ЗАКАЗЧИКА

Избавление от:

- Необходимости вникать в технические процессы;
- Проблем с выбором решения и его закупкой;
- Внедрения и сопровождения работы 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.



INFOSECURITY

a Softline company

gk-is.ru