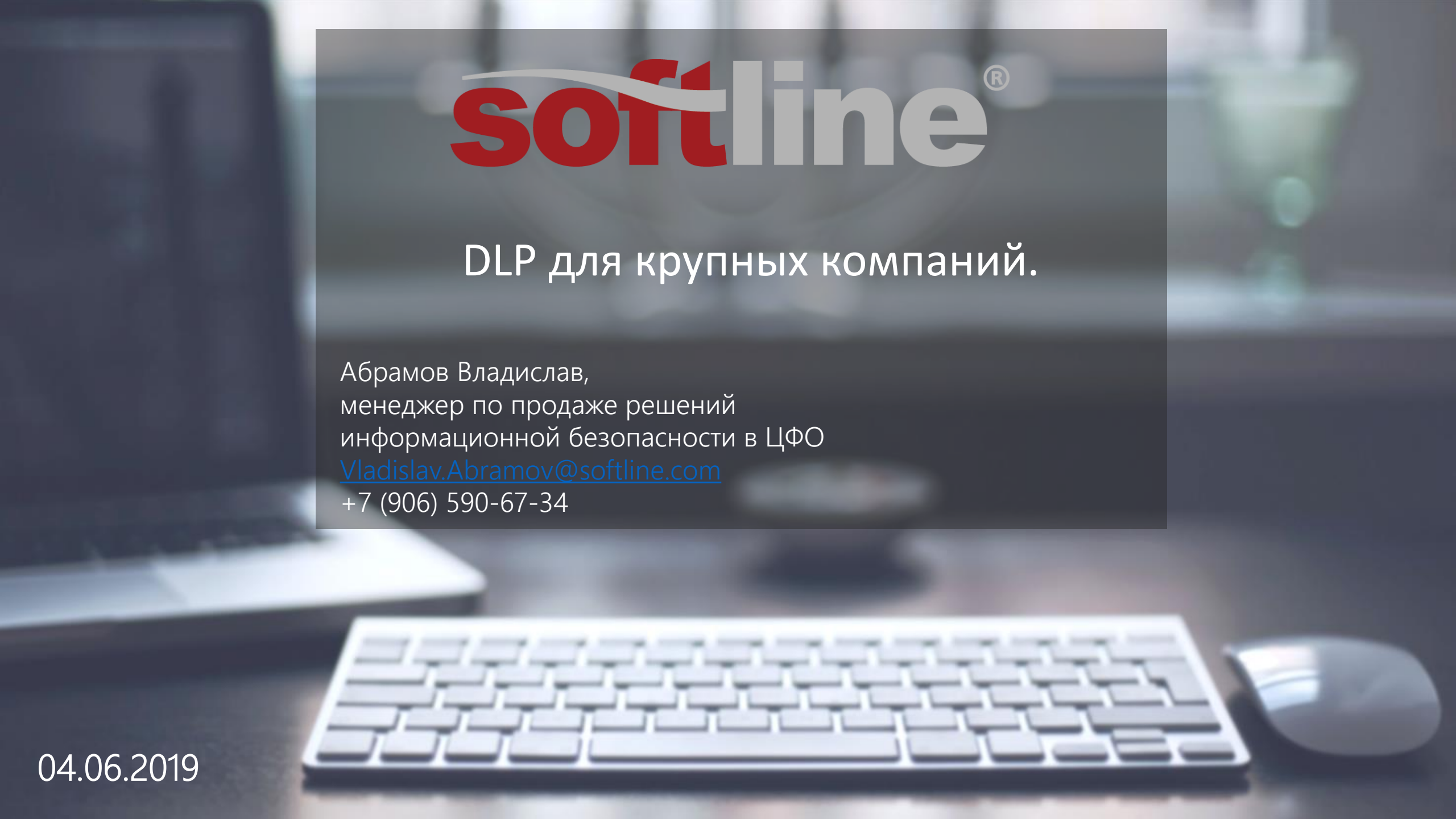


DLP для крупных компаний.

Абрамов Владислав,
менеджер по продаже решений
информационной безопасности в ЦФО
Vladislav.Abramov@softline.com
+7 (906) 590-67-34

04.06.2019

Законодательство в сфере утечек данных

Основные законы:

- 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Указ Президента №188 «Об утверждении перечня сведений конфиденциального характера»
- 152-ФЗ «О персональных данных»
- 98-ФЗ «О коммерческой тайне»

Ст. 272 УК РФ: неправомерный доступ к информации (н-р, копирование информации, охраняемой законом)- срок **до 2 лет**

Ст. 183 УК РФ: разглашение или использование сведений, составляющих коммерческую тайну, причинившее крупный ущерб, - срок **от 3-5 лет**

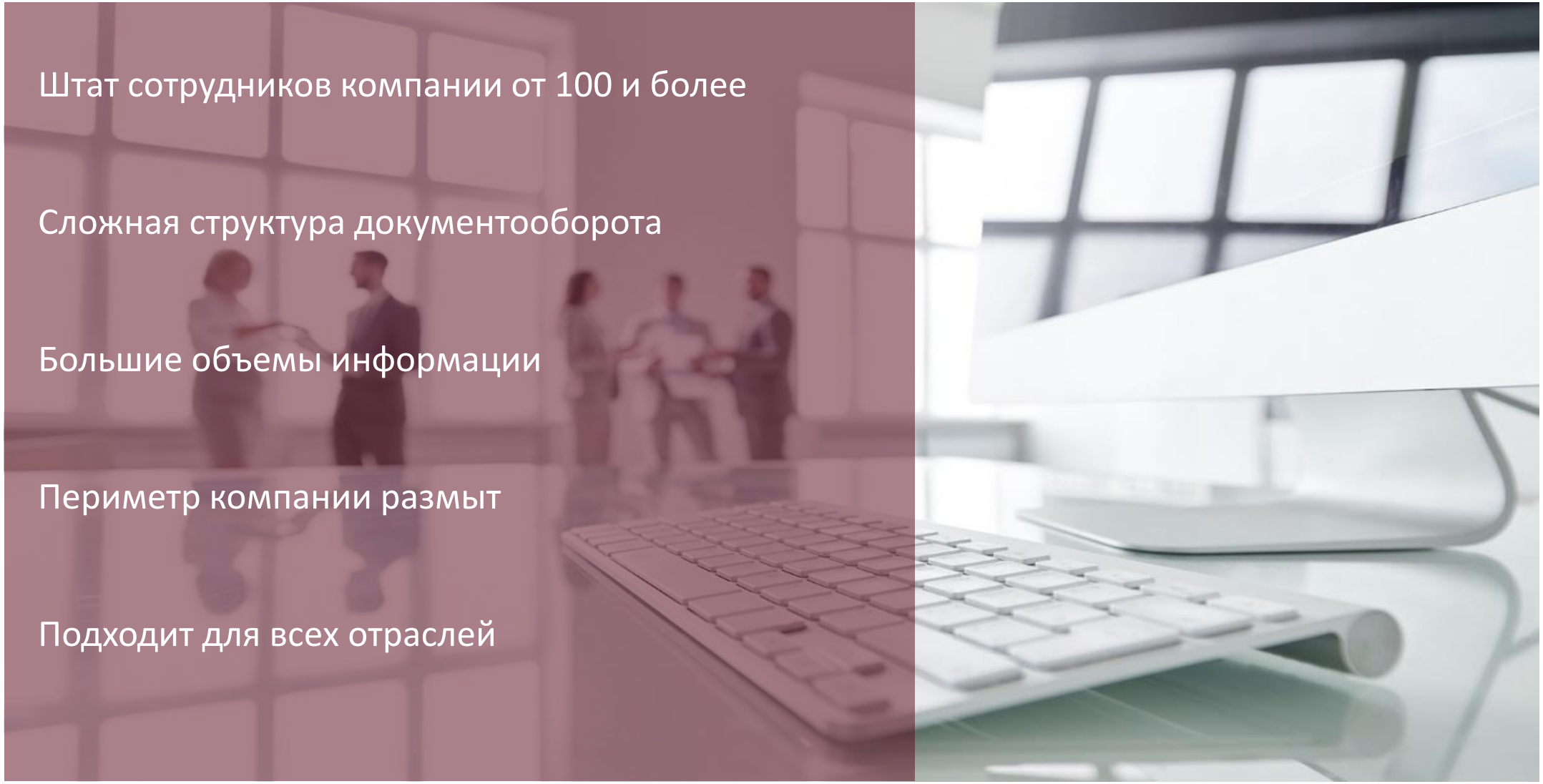
Основные требования и рекомендации регуляторов:

- Приказ ФСТЭК №21 (ПДн)
- Приказ ФСТЭК №17 (государственные информационные системы)
- СТО БР ИББС (банки)
- 382-П (НПС)
- PCI DSS (платежные системы)

Прочие рекомендации:
ISO 27001/ISO 27002 (ГОСТ 27001/ГОСТ 17799)

Ст. 13.11.3 КоАП РФ: утечка ПДн в случае их обработки в АСУ, - штраф 100 000 – 200 000 рублей

Особенности компании



Штат сотрудников компании от 100 и более

Сложная структура документооборота

Большие объемы информации

Периметр компании размыт

Подходит для всех отраслей

Задачи, решаемые DLP помимо зашиты от утечек конфиденциальных дынных

1. Проведение расследований инцидентов информационной безопасности.
2. Инструмент управления рисками.
3. Соответствие требованиям регуляторов: КТ, ПДн, банковская тайна.
4. Обеспечение безопасности бизнес-процессов.

Кому поможет DLP-система

Собственники бизнеса, ТОП-менеджмент

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

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

ИБ

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

Функциональные руководители / HR

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

Кейсы. Утечки данных с рабочих станции.

Злоумышленник	Сценарий
Сотрудник отдела бухгалтерии	Сотрудник решил скопировать на личный USB-носитель данные анкет с персональными данными клиентов. ФЗ №152 «Защита персональных данных»

Ущерб
Репутационные риски

Кейсы. Утечки данных с рабочих станции.

Злоумышленник	Сценарий
Инженер на производстве	Сотрудник решил продать проектную документацию.

Ущерб
Потеря интеллектуальной собственности организации

Кейсы. Утечки данных через мобильные устройства

Злоумышленник	Сценарий
Топ-менеджер PNC Bank Эйлин Дейли	**Фотографировала экран** своего компьютера со стратегической информацией на смартфон незадолго до увольнения

Ущерб
По оценкам PNC Bank, ущерб от действий бывшего топ-менеджера составил **250 млн. $**

Просто цифры...
(первое полугодие 2018 года)

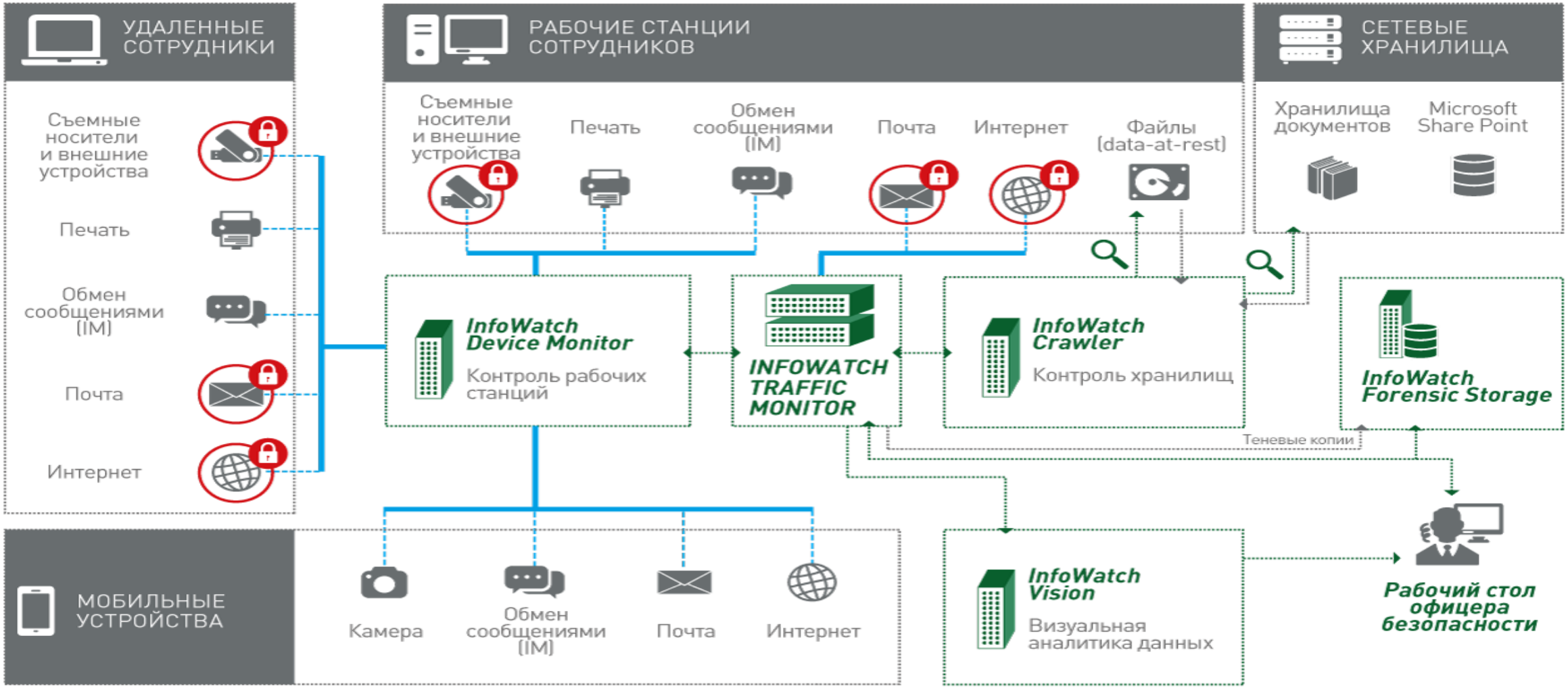
1. Обнародован 1039 случай утечки конфиденциальной информации, что на 12% превышает количество утечек за аналогичный период 2017 года.
2. Скомпрометировано 2,39 млрд. записей персональных и платежных данных.
3. Внешние атаки стали причиной 35,5% утечек данных. В 64,5% случаев утечка данных произошла под воздействием внутреннего нарушителя.
4. Зафиксирована 21 «мега-утечка». В результате каждой «утекло» более 10 млн записей. На «мега-утечки» пришлось 97% совокупного объема скомпрометированных записей.
5. В 53,5% случаев виновными в утечке информации оказались штатные сотрудники компаний. Более чем в 2% случаев — высшие руководители организаций и иные привилегированные пользователи.

* По данным Аналитического центра InfoWatch

Схема работы DLP-системы

Технологий анализа контента

Схема работы DLP-системы (пример)



Новые горизонты

- Функциональность контроля эффективности сотрудников.
- Функциональность User Behavior Analytics (UBA).
- SOC DLP

Результаты внедрения DLP системы

1.Контроль за движением конфиденциальной информации и ее защиту:

Защита от утечки коммерческой тайны;

Защита интеллектуальной собственности;

Предотвращение утечек персональных данных и баз данных;

2. Контроль доступа сотрудников к конфиденциальной информации;

3. Выявление злоумышленников, лиц, занимающихся промышленным шпионажем, а также привлечение их к ответственности за нарушения.

Реализованные проекты Softline

- Forcepoint DLP (Websense AP-DATA)
- Infowatch Traffic Monitor
- Solar Security Dozor
- Symantec
- Falcongaze
- McAfee

И другие.

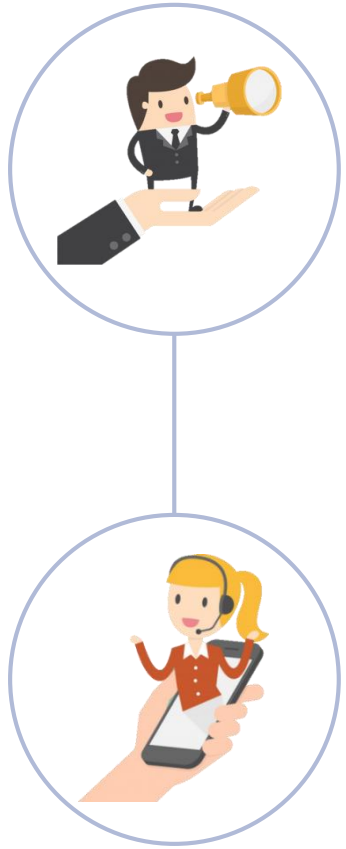
DLP как сервис

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

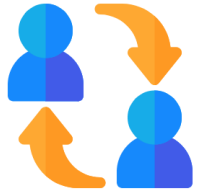


Этапы реализации

Выявление потребностей и определение SLA

Подписание NDA

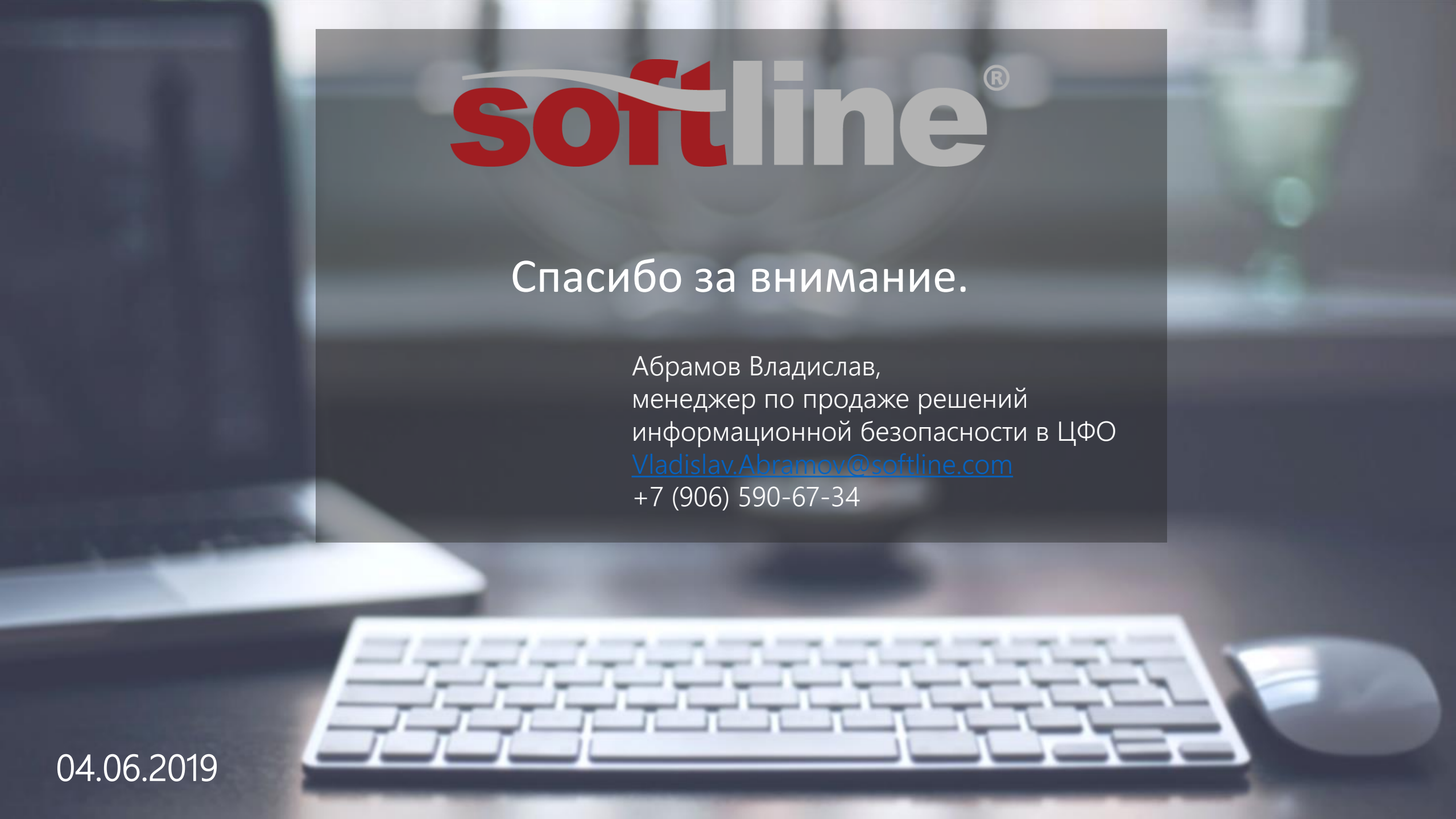
Согласование доступов и учетных записей



Обмен информацией

Возражения и работа с ними

Возражения	Ответы
Доступ к критичной информации	Регулярные проверки сотрудников на полиграфе, в т.ч. «по запросу» заказчика; Настройка ограниченного доступа / списки исключений; 8 лет безупречной репутации (соблюдение NDA);
Мы становимся Вашими заложниками	Вы имеете доступ ко всем хранилищам информации и можете самостоятельно проверять достоверность предоставляемой информации.
Слишком дорого	Калькулятор для расчета стоимости = гибкость. Потери от инцидента могут быть фатальны для компании. Нет проблем с наймом и содержанием в штате собственной команды аналитиков, а их очень сложно искать.
Зачем тогда нам СБ и ИБ?	Отлаженный процесс взаимодействия с СБ/ИБ - дополняем, а не заменяем. Повышается эффективность и результат работ. Они смогут освободить свои ресурсы и заняться другими важными задачами.
Куда мы теперь денем нашу DLP? Она вам не подойдет?	Имеем опыт работы со всеми представленными на рынке отечественными DLP-системами, знаем их сильные и слабые стороны.



Спасибо за внимание.

Абрамов Владислав,
менеджер по продаже решений
информационной безопасности в ЦФО
Vladislav.Abramov@softline.com
+7 (906) 590-67-34

04.06.2019