Практические кейсы применения DLP в деятельности структурных подразделений компании

Саматов Константин Михайлович

Член Правления

Ассоциация руководителей служб информационной безопасности

Что понимается под DLP?

- DLP (Data Leak Prevention)
- UAM (User Activity Monitoring), Employee monitoring
- UEBA (User and Entity Behavior Analytics)

Дисклеймер: приведенные в презентации кейсы не имеют отношение к текущим работодателям автора

Структурные подразделения в организации, которым может быть полезна DLP

- Руководство (менеджмент различных уровней)
- Информационная безопасность
- Служба безопасности
- Подразделение кадров (HR)
- Финансовые подразделения
- Подразделение маркетинга и продаж
- Юристы

Кейс: Юристы

Применение DLP в финансах, маркетинге и продажах

- Защита финансовых данных и маркетинговых материалов
- Контроль за конфиденциальностью маркетинговых стратегий
- Предотвращение утечек рекламных кампаний
- Предотвращение случайной отправки информации контрагентам которым она не предназначена

Кейс: Продажники

Применение DLP в подразделении кадров

- Защита чувствительных данных о сотрудниках
- Предотвращение утечки личных данных
- Контроль лояльности работников
- Контроль соблюдение правил внутреннего распорядка
- Контроль лояльности работников

Кейс «Лояльность работников»

Поиск нового места работы

Прокрастинация

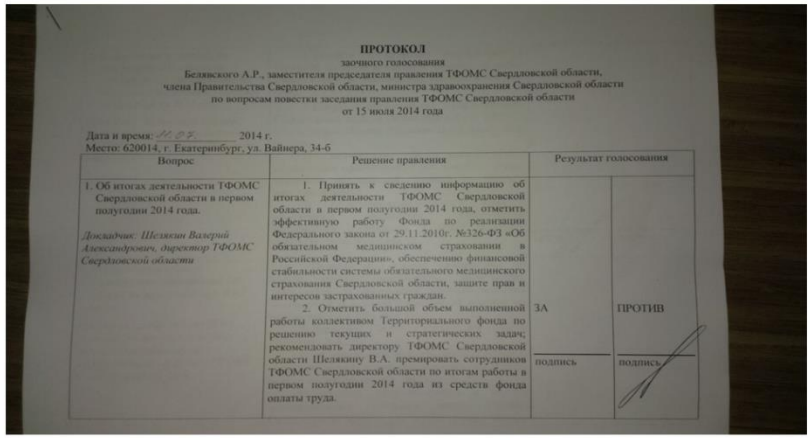
Работа на нескольких работодателей

Применение DLP в ИБ

- Защита чувствительных данных
- Предотвращение утечки данных
- Выявление угроз безопасности
- Выявление событий ИБ
- Расследование событий ИБ

Кейс «Крот»

На сайте URA.RU была размещена статься, в которой был представлен протокол совещания.

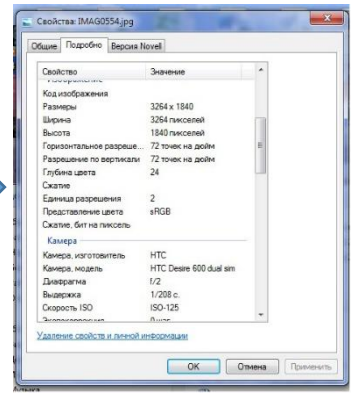


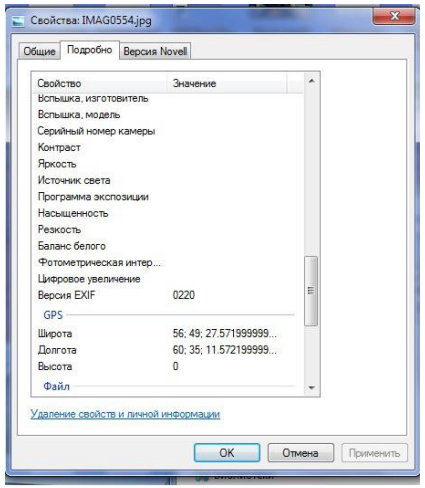
ПРОТОКОЛ
заочного голосования
Белявского А.Р., заместителя председателя правления ТФОМС Свердловской области,
члена Правительства Свердловской области, министра здравоохранения Свердловской области
по вопросам повестки заседания правления ТФОМС Свердловской области
от 15 июля 2014 года

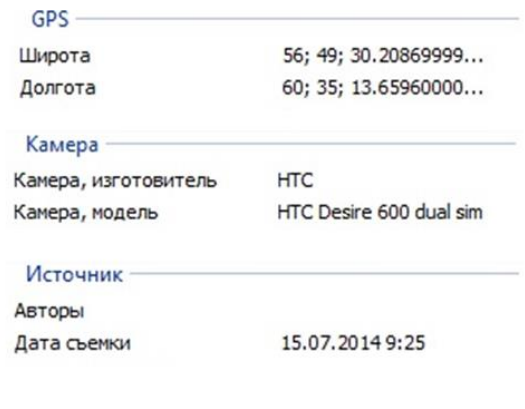
Дата и время: 15.07. 2014 г.
Место: 620014, г. Екатеринбург, ул. Вайнера, 34-б

Вопрос	Решение правления	Результат голосования	
1. Об итогах деятельности ТФОМС Свердловской области в первом полугодии 2014 года. *Докладчик: Шелякин Валерий Александрович, директор ТФОМС Свердловской области*	1. Принять к сведению информацию об итогах деятельности ТФОМС Свердловской области в первом полугодии 2014 года, отметить эффективную работу Фонда по реализации Федерального закона от 29.11.2010г. №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», обеспечению финансовой стабильности системы обязательного медицинского страхования Свердловской области, защите прав и интересов застрахованных граждан. 2. Отметить большой объем выполненной работы коллективом Территориального фонда по решению текущих и стратегических задач; рекомендовать директору ТФОМС Свердловской области Шелякину В.А. премировать сотрудников ТФОМС Свердловской области по итогам работы в первом полугодии 2014 года из средств фонда оплаты труда.	ЗА подпись	ПРОТИВ подпись

По внешним признакам можно определить, что документ уже был копией, т.к. и дата и подпись черного цвета.



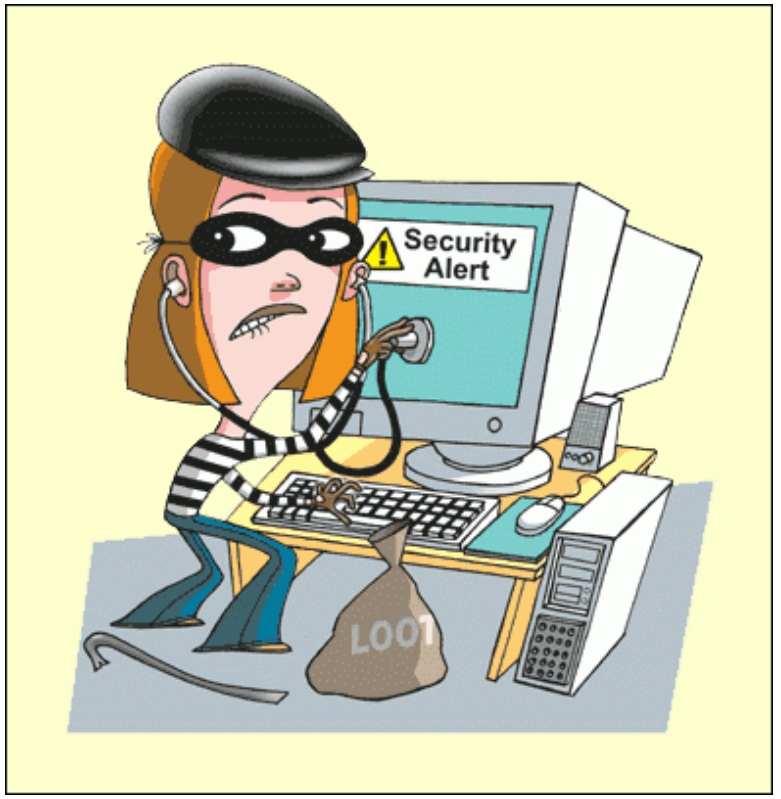




Применение DLP в СБ

- Выявление противоправных действий работников
- Предотвращение утечки
- Контроль лояльности работников
- Контроль соблюдения правил внутреннего распорядка
- Прогнозирование угроз внутреннего нарушителя
- Сбор фактуры (доказательной информации, компрометирующих данных и т.п.).

Кейс «Путана»

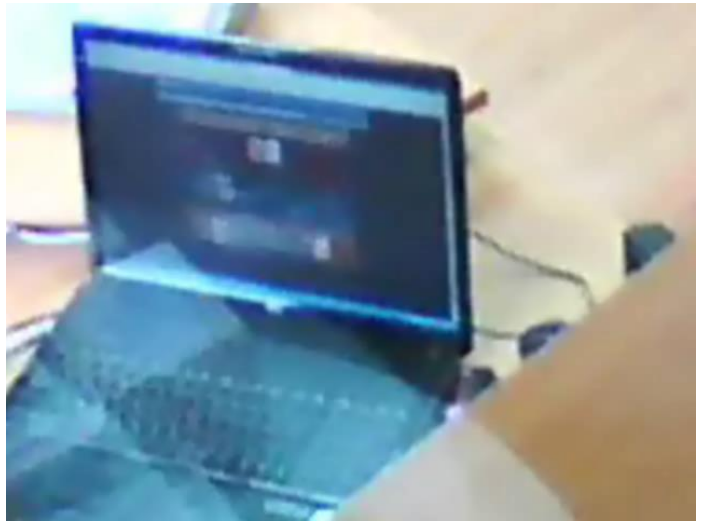


Применение DLP Менеджментом

- Информация чем заняты сотрудники
- Контроль внутреннего распорядка
- Удержание нужных людей
- Распределение по проектам/задачам

Кейс «Бездельник»

1. Тестирование камер видеонаблюдения для филиалов



2. Побочный результат: появились подозрения на то, что не все сотрудники уделяют должное внимание исполнению своих служебных обязанностей. Было решено поставить круглосуточное видеонаблюдение за **рабочим местом** одного из сотрудников. Также был осуществлен анализ сетевого трафика с IP адреса объекта и анализ истории его веб браузера.

3. Результаты контроля Любимая игра

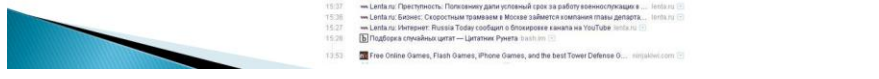
Демотиваторы

Активность веб браузера данного сотрудника

Тяжела и неказиста жизнь простого программиста

13 самых сомнительных секс-рекордов (13 фото)

Сиськи и котики (40 фото)



ВОПРОСЫ?

Саматов Константин Михайлович

Член Правления

Ассоциация руководителей служб информационной безопасности