ИНФОСИСТЕМЫ ДЖЕТ

Контроль действий ИТ-администраторов как важная мера противодействия утечкам данных

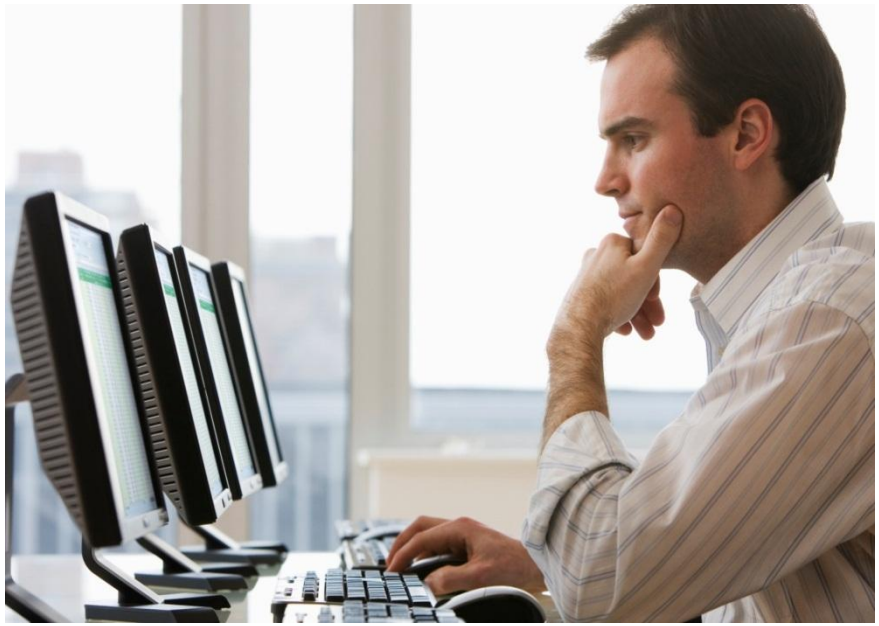
для DLP-Russia 2011

Кирилл Викторов, заместитель директора по развитию бизнеса компании «Инфосистемы Джет»

Свой среди чужих

Технически подготовленный инсайдер

- Знает архитектуру сети (VLANы, адресные пространства, коммутация)
- Понимает организацию шлюза доступа в Интернет
- Располагает информацией о системах защиты
- Владеет учетными записями администратора на серверах и рабочих станциях



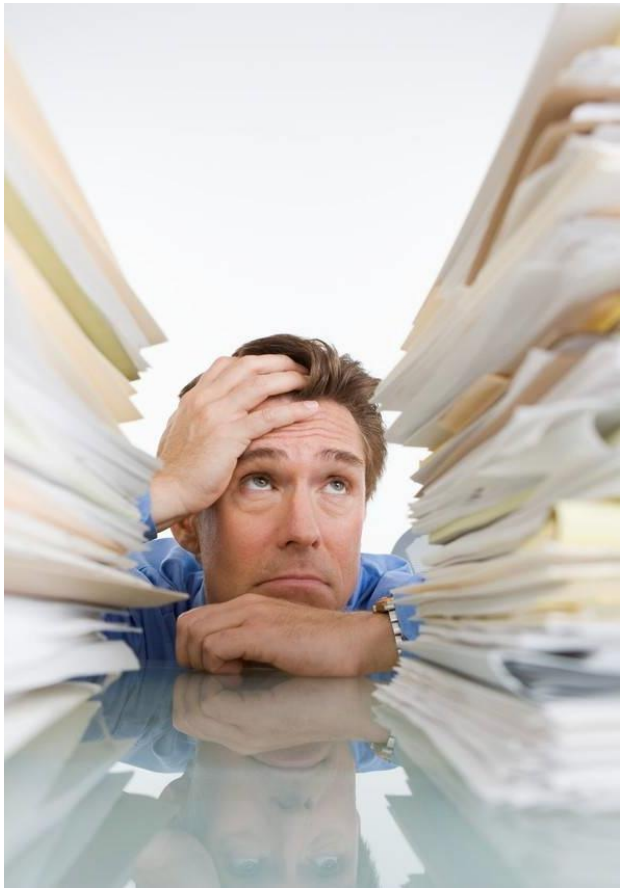
А если он «снаружи» компании,

NDA или СОК **BS7799-2 или ISO27001**

- то ваши источники информации сильно ограничены

Как расследовать инциденты?

- Большой объём информации
  - неструктурированной, из разных источников;
  - не всегда понятно, что искать (нет модели нарушителя);
- Человеческий фактор
  - вычитывать несколько Мб журналов в день – нереально;
  - принятие решений – субъективно



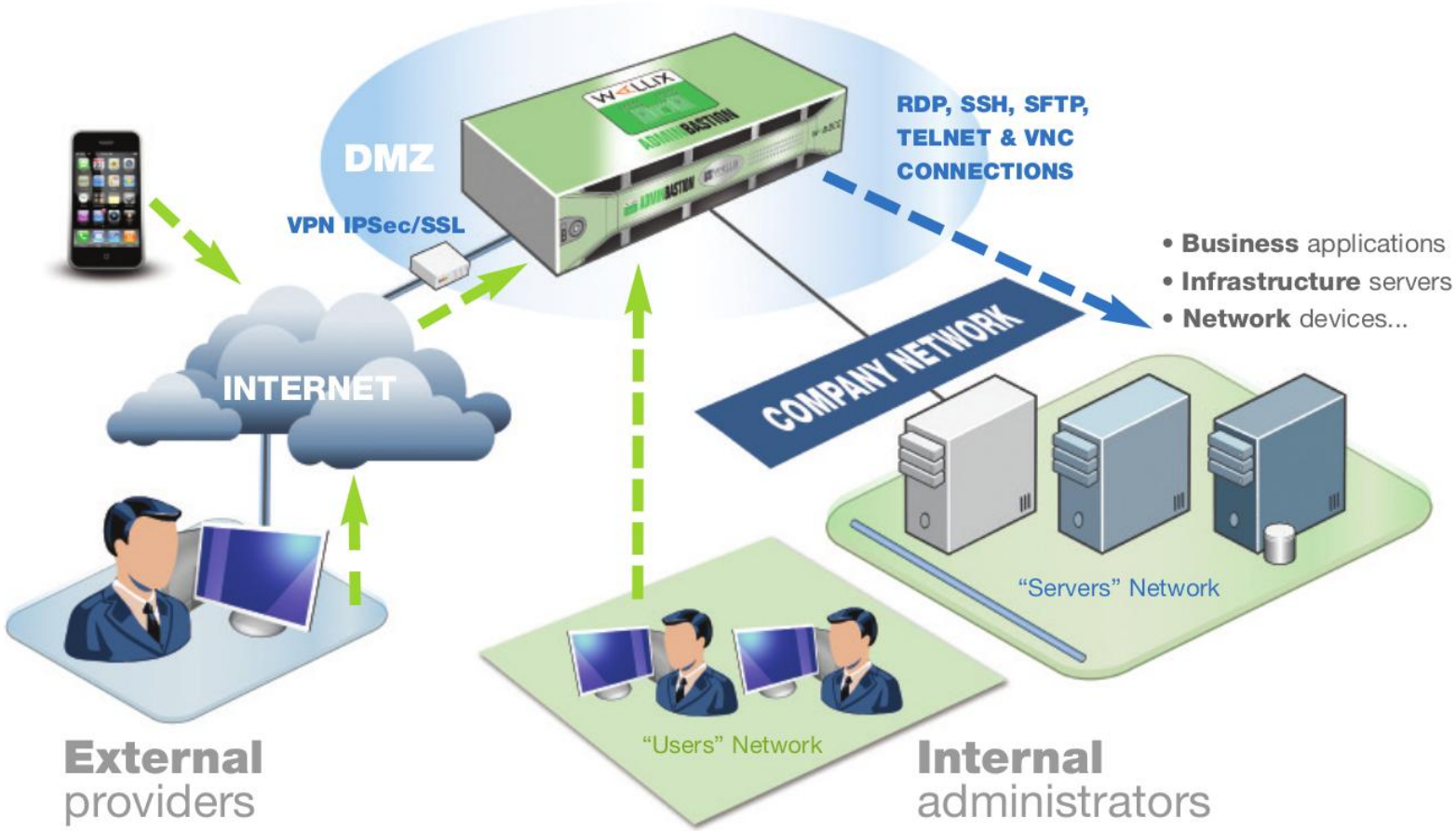
Есть ли требования у регуляторов?

- Удаленный доступ к критически важным системам должен контролироваться и фиксироваться
- Аудит и проверка критически важных IT- систем должны производиться непрерывно
- Записи аудита необходимо сохранять для дальнейшего анализа

Идея

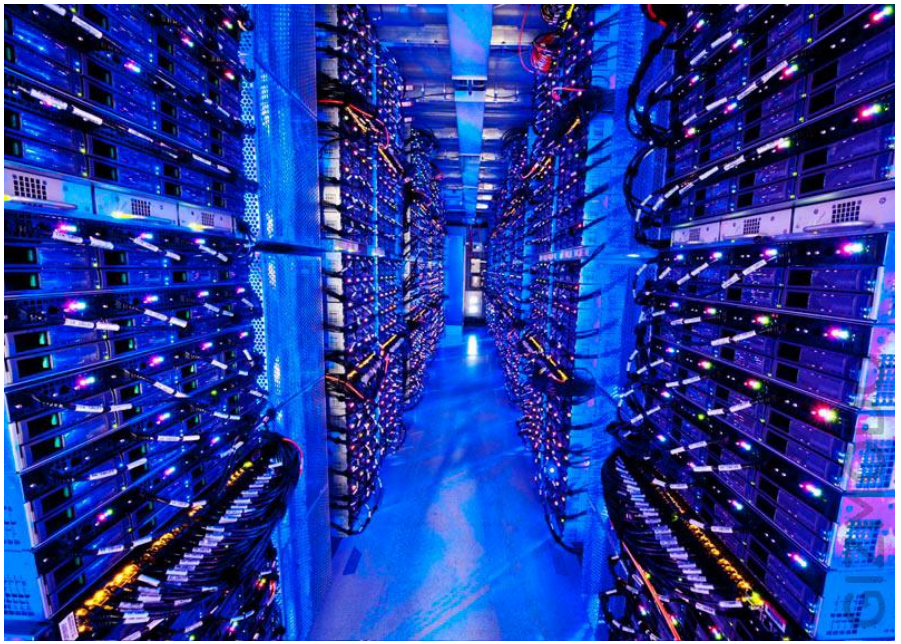
Wallix AdminBastion – реализация

Wallix AdminBastion – корпоративное решение **для контроля и аудита действий, выполняемых на информационных системах**



1. Управление серверами

- Кто и какие действия выполнял на сервере?
- Что делают системные администраторы?
- К каким ресурсам получил доступ аудитор?



2. Управление инфраструктурой

- Разграничение доступа к критически важным серверам
- Проверка лояльности администраторов систем
- Контроль всех действий на управляемых серверах

3. Контроль внешнего IT аутсорсинга

- Оценка эффективности и качества внешнего аутсорсинга (SLA контроль)
- Контроль доступа к критически важным серверам
- Расследование инцидентов

- Проверка проведения профилактических и регламентных работ

4. Контроль терминальных серверов

- Контроль действий администраторов на сервере
- Управление доступом пользователей не только средствами сервера
- Аудит действий пользователей при необходимости

Оценка стоимости

Число устройств администраторов	Наличие HA, встроенного в ПО	Возможность виртуализации	Стоимость решения (ПО + внедрение + 1 год техподдержки)
25	Да	Есть	125 000
50	Да	Есть	160 000
100	Да	Есть	220 000
200	Да	Есть	290 000

Поддержка вендора предусматривает реакция на запрос течение 24 часов.

Спасибо за внимание!