



**ПОЛИКОМ** ПРГ

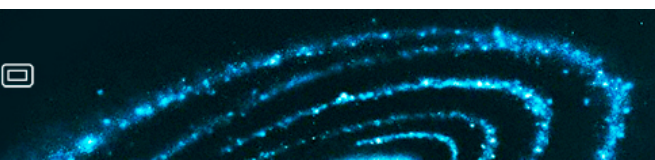
Созвездие высоких технологий

Требуется ли внедрение DLP-решения изменения структуры процессов компании ?

Орешин Михаил

# Схожесть ведения проектов по DLP и СЭД

- Схожесть ведения проектов по DLP и СЭД.
  - В обоих случаях отдел информационной безопасности (как инициатор) или отдел IT (как эксплуатант) не смогут удачно завершить проект не используя ресурс тех, кто этой информацией живет !!!



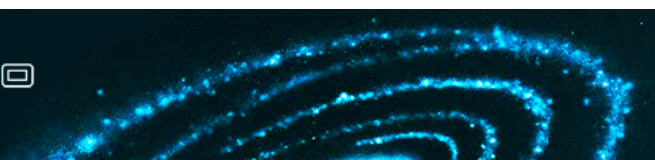
## Перед началом внедрения ответить на вопросы:

- Для кого внедряем ? Почему внедряем ?
  - Требования регулятора
  - Инцидент
  - Внедрения КСУИБ
- В зависимости от этого разные спонсоры и заказчики.



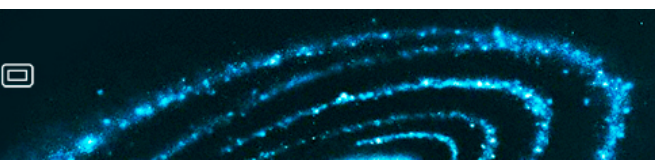
## Первый процесс :

- Первый процесс, который точно придется внедрять в компанию при использовании DLP. Это рутинный каждодневный процесс контроля утечек информации из компании с использованием выбранного решения. Банально но факт.



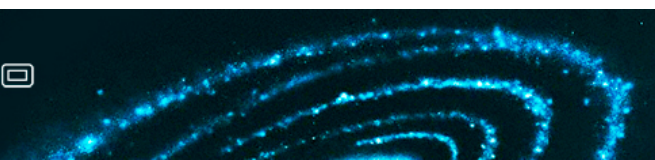
# Классификация данных:

- Стратегические: Данные критичные для бизнеса, данные за которыми следят регуляторы (персональные данные).
- Тактические: Данные, которая компания сама определяет как коммерческая тайна (финансовую информа-цию, планирующиеся маркетинговые программ, внутренний документооборот) или данные которые связаны соглашением конфиденциальности с внешними контрагентами. Ключевое что данные хранятся в каких-либо защищенных системах (СЭД, Портал, базы данных etc)



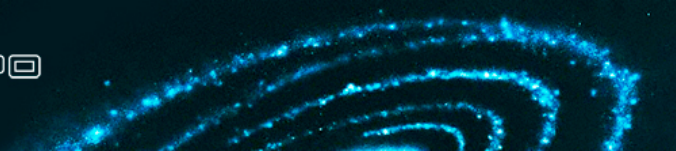
# Классификация данных:

- Оперативные: неформализованные и неконсолидированные чувствительные данные, создающиеся и изменяющиеся вне защищенных корпоративных систем.
- Парадокс. Данные которые по сути своей являются тактическими или даже стратегическими, хранятся могут как оперативные.



# Основные причины неудачи:

- Отсутствие четкого понимания объекта защиты
- Ориентация на функционал решения
- Ориентация только на внутренние ресурсы и опыт
- Давление на бизнес
- Отсутствуют критерии успешности проекта



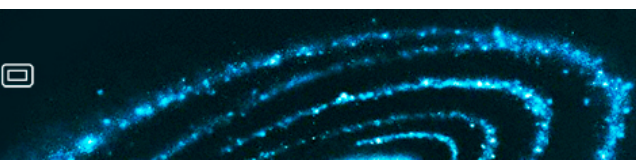
# Пример - проектные институты (или организации ведущие проектную деятельность). :

*Пример не относится к конкретному институту. Это консолидированная информация.*

Проблематика:

Основные каналы утечек

- 1) исходные данные по старым объектам
  - a. прямое воровство исходных материалов на бумажных носителях (неучтенные или даже учтенные экземпляры)
  - b. несанкционированное копирование и фотокопирование
- 2) свежие материалы
  - a. копирование на флешках и CD/DVD из файловых архивов
  - b. «левые» копии на принтерах и плоттерах
  - c. Несанкционированные файловые и CD/DVD архивы на рабочих местах (из-за недостаточности или отсутствия процедур резервного копирования)
  - d. Воровство сисадминами незашифрованных баз и архивов

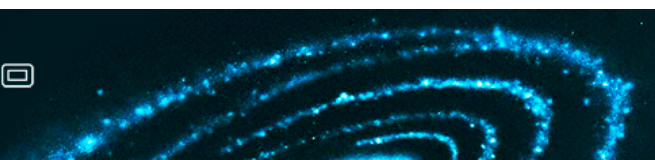




# Пример - проектные институты (или организации ведущие проектную деятельность). :

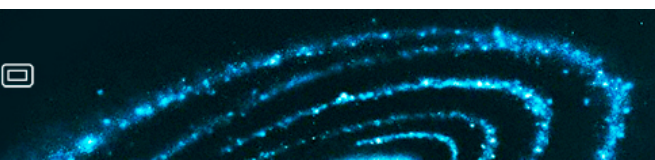
Решение:

- Организационные мероприятия по инвентаризации и наведения порядка в архиве проектно-конструкторской документации
- Организационные мероприятия в сети предприятия
  - Выявление архивов, имеющих коммерческую ценность
  - Закрытие или контроль CD/DVD и USB портов
  - Разделение функций системного администрирования и безопасности
  - Внедрение электронного архива



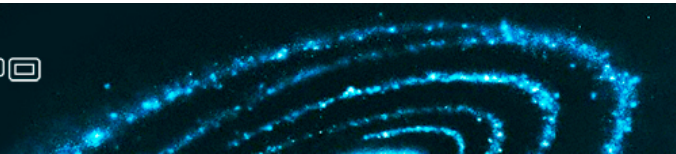
# Пример - проектные институты (или организации ведущие проектную деятельность). :

- Организационные мероприятия по инвентаризации и наведения порядка в архиве проектно-конструкторской документации
- Организационные мероприятия в сети предприятия
  - Выявление архивов, имеющих коммерческую ценность
  - Организация централизованного резервного копирования и быстрого восстановления этих ресурсов, удобного для пользователей
  - Закрытие CD/DVD и USB портов
  - Разделение функций системного администрирования и безопасности
  - Внедрение электронного архива



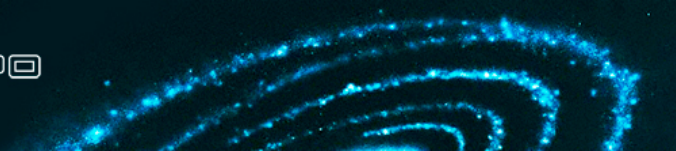
# Основные причины неудачи:

- Отсутствие четкого понимания объекта защиты
- Ориентация на функционал решения
- Ориентация только на внутренние ресурсы и опыт
- Давление на бизнес
- Отсутствуют критерии успешности проекта



# Выводы:

- Внедрение DLP системы может привести к изменению текущих процессов, но только в случае если они уже есть – формализованы и прописаны
- Попытка кардинально изменить текущие процессы скорее всего приведут к срыву внедрения
- Внедрение DLP системы хорошо соотносится с внедрением или реинжиниринге процессного управления в компании





**ПОЛИКОМ** ПАО

Созвездие высоких технологий

# Благодарим за внимание!

Москва	+7 (495) 232 -2920
Санкт-Петербург	+7 (812) 325 8400
Челябинск	+7 (351) 266 1794
Череповец	+7 (8202) 58 7781

[www.polikom.ru](http://www.polikom.ru)