# Мы купили DLP...

и понеслось....

Пиргалина О.Л. Офицер информационной безопасности.
АО «Евразийский Банк»

# Что такое DLP?

Может быть как агентским, так и граничным

Защищает от всех типов угроз

Позволяет искать данные при хранении

Блокирует передачу данных

Решение из коробки


Не дает ложных срабатываний

Позволяет распознавать графику

Анализирует информацию

Может читать всю зашифрованную информацию

Требует длительной настройки правил и политик

Позволяет просматривать всю почту пользователей

Не влияет на нормальную работу пользователя

Анализирует атрибуты передачи информации

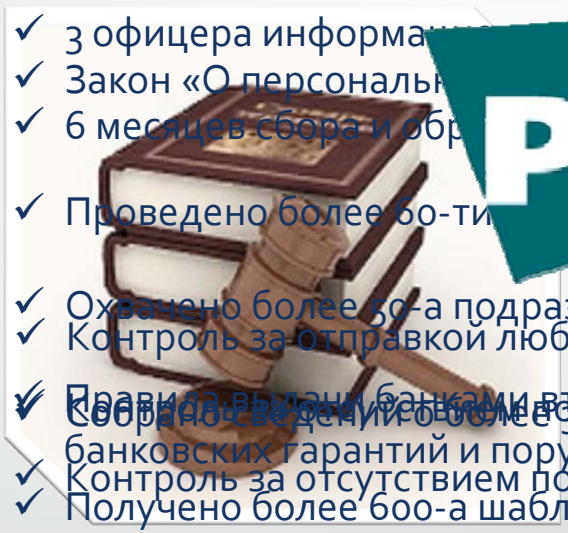
# Что такое DLP?

Вам пора задуматься о внедрении DLP, если Вам нужен инструмент:

- ✓ выполнения регуляторных требований
- ✓ анализа и изменения поведения пользователя
- ✓ автоматизации процесса реагирования на события
- ✓ инвентаризации конфиденциальных данных
- ✓ выявления нарушений бизнес-процессов
- ✓ блокировки утечек информации

# Кто знает, что защищать?

Бизнес подразделения

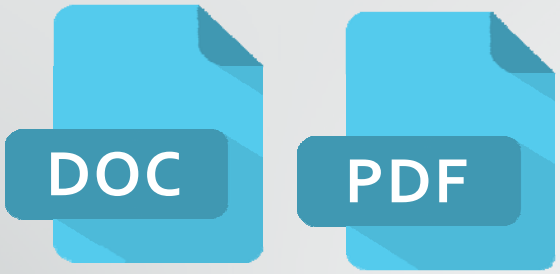


- ✓ 3 офицера информа… …ости
- ✓ Закон «О персональн… …щите».
- ✓ 6 месяцев сбора и обр…
- ✓ Проведено более 60-ти…
- ✓ Охвачено более 50-а подразделен…
- ✓ Контроль за отправкой любых дан… …ив сегмента процессинга
- ✓ Правила выдачи банками второго у… …
- ✓ Собрано сведений обо более 300-а бизнес… банковских гарантий и поручительств
- ✓ Контроль за отсутствием полных номеров карт в хранилищах
- ✓ Получено более 600-а шаблонов конфиденциальной информации

Требования регуляторов


Международные стандарты

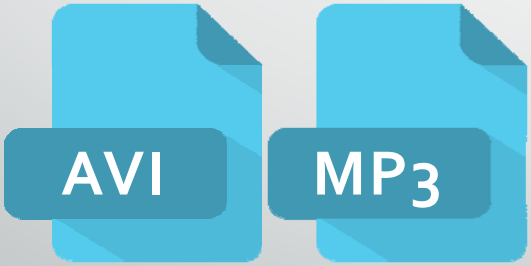
# Что ловим?




- ✓ Типовые договора
- ✓ Шаблоны выписок
- ✓ Форматы счетов


- ✓ Конфигурационные файлы
- ✓ Файлы журналов событий
- ✓ Аутентификационные данные


- ✓ Отчеты
- ✓ Калькуляторы




- ✓ Поиск по атрибутам


- ✓ Поиск по формату файла

# Где ловим?

Email

WWW (HTTP(S))

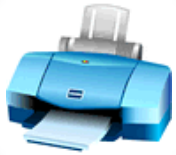
Съемные носители

CD/DVD

Буфер обмена

HDD

Общие папки



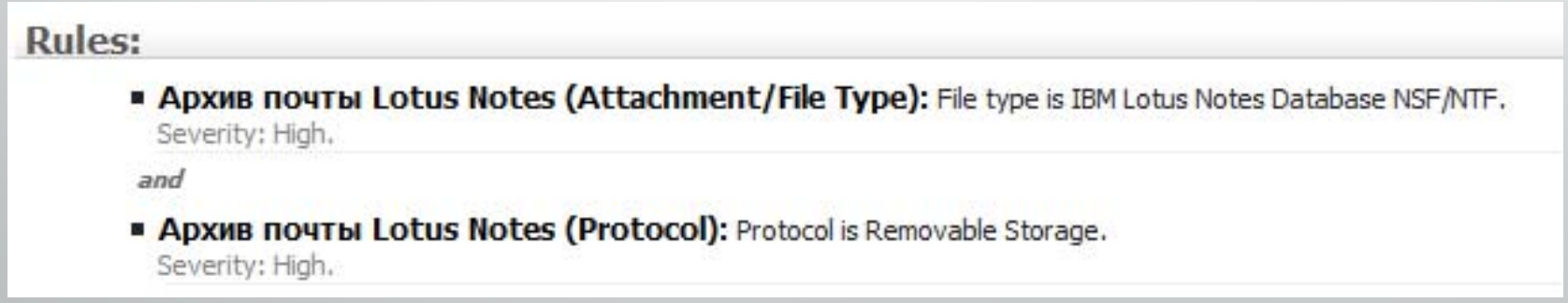
Принтер/факс

# Вся соль в правилах!

Правило строится по нескольким критериям:

- содержимое (регулярные выражения, ключевые слова, идентификаторы, отпечатки и.тд.);
- атрибуты (размер файла, тип файла, название файла);
- протоколы и способы передачи данных (smtp, http, ftp, буфер обмены, принтер и т.д.);
- количество совпадений содержимого для срабатывания (например, если больше 100-и)

Чем больше количество уточняющих критериев, тем меньше будет ложных срабатываний.



# Вся соль в правилах!

**Rules:**

- **Ключевые слова (Keyword Match):** Match "sys", "system", "root".
  Severity: High. Count all matches. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

*and*

- **Ключевые слова (Keyword Match):** Match "Пароль", "pass", "password", "passwd".
  Severity: High. Count all matches. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

*or*

- **Пароли (Keyword Match):** Match "Пароль", "pass", "passwd", "password", "Qq123456", ....
  Severity: High. Count all matches. Look in subject, body, attachments. Case insensitive. Match on whole words only.

*and*

- **Пароли (Keyword Match):** Match "login", "логин".
  Severity: High. Count all matches. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

*or*

- **Password Filenames (Attachment/File Name):** Match passwd, shadow.
  Severity: High.

*or*

- **/etc/passwd Format (Regular Expression):** Match "\w{1,30}:[^:]{1,30}:\d{1,30}:\d{1,30}:[-a-zA-Z'()\s]{0,30}:(/\w{0,30}){0,30}:(/\w{0,30}){0,30}".
  Severity: High. Count all matches. Look in envelope, subject, body, attachments.

*or*

- **/etc/shadow Format (Regular Expression):** Match "\w{1,30}:[^:]{0,30}:\d{1,30}:\d{1,30}:\d{1,30}:\d{1,30}:\d{0,30}:\d{0,30}:\d{0,30}".
  Severity: High. Count all matches. Look in envelope, subject, body, attachments.

*or*

- **SAM Passwords (Regular Expression):** Match "[-a-zA-Z_0-9$]{1,30}:\d+:[a-zA-Z_0-9*\s]{32}:[a-zA-Z_0-9*\s]{32}:".
  Severity: High. Count all matches. Look in envelope, subject, body, attachments.

# От правил к политикам!

Правила объединяются в политики следующим образом:

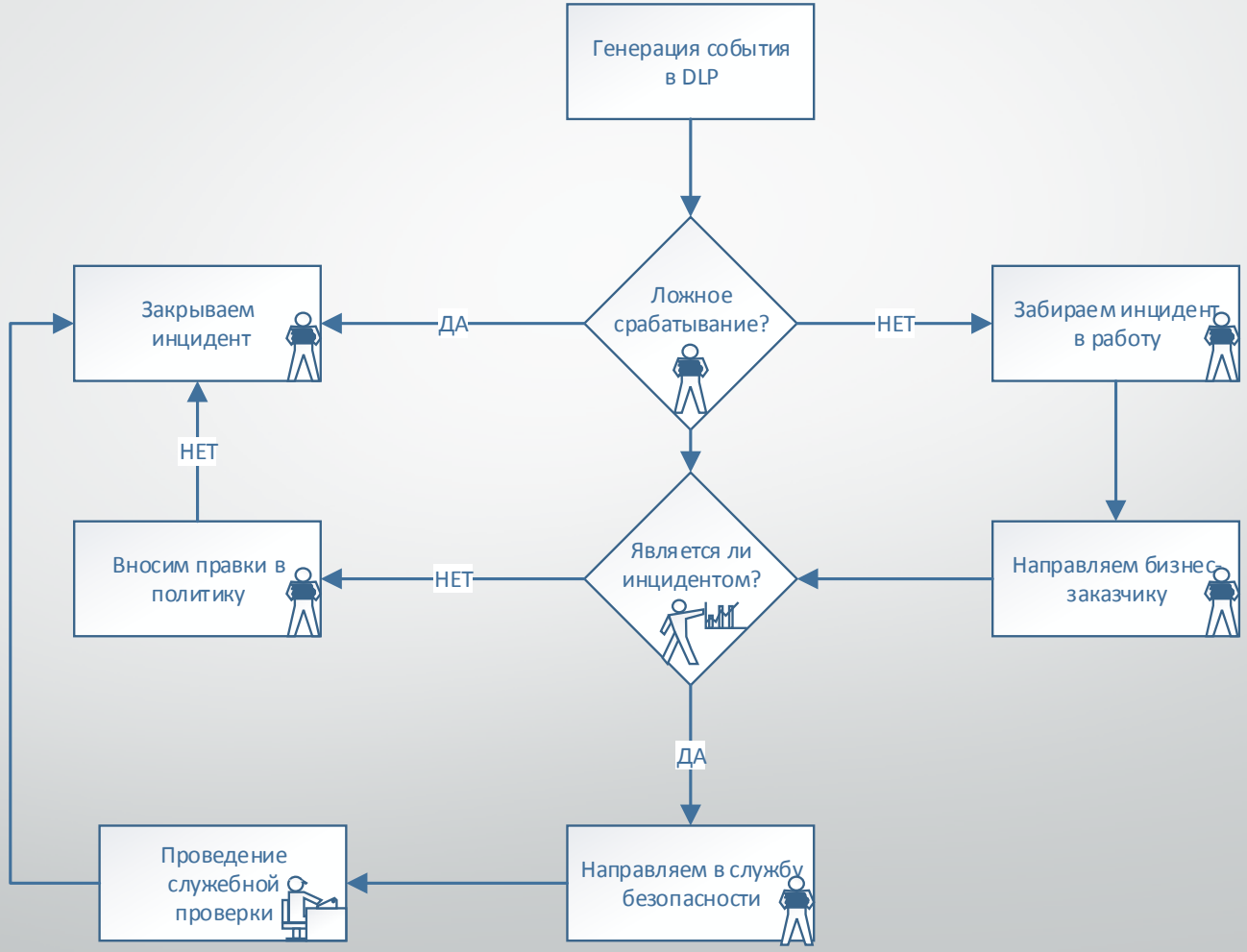
- ✓ Политике назначается имя, вводится описание и бизнес-заказчик
- ✓ Вводятся правила детектирования конфиденциальной информации
- ✓ Вводятся группы, к которым применима данная политика
- ✓ Вводятся исключения из информации, попадающей под правила детектирования
- ✓ Вводятся исключения из групп, к которым применима данная политика
- ✓ Вносятся действия, по реагированию на срабатывание (запись, установка статуса и т.д.)

# А был ли инцидент?

Бизнес владелец

Офицер ИБ

Работник СБ



# Что в итоге у нас получилось…

- ☑ Внедрено более 30 политик, написано более 200 правил
- ☑ Обработано за текущий год более 60 000 срабатываний
- ☑ Количество срабатываний за последние 30 дней менее **3500** при среднем значении **6000**
- ☑ Доля срабатываний по агентам составляет около 75%, по сети менее 24%
- ☑ Разбором событий и оптимизацией правил занимаются 3 работника
- ☑ Временные затраты каждого работника не менее 2-х часов ежедневно
- ☑ Количество "ложных" срабатываний по политикам снижен с 85% до 45%
- ☑ Подтвержденных инцидентов более 200, уволено 2 работника

# И еще пара советов

- ☑ Своевременно обрабатывать события и реагировать на инциденты
- ☑ Автоматизировать всё, что можно автоматизировать
- ☑ Указывать в описании политики контактное лицо по подтверждению инцидентов
- ☑ Используйте больше «заточенных» политики и меньше общих
- ☑ Не бойтесь пользоваться идентификаторами и регулярными выражениями
- ☑ Помните, что необходимо искать информацию, а не файл
- ☑ Используйте различные механизмы анализа содержимого, для разного типа информации
- ☑ Выделите для разбора событий отдельного человека с полной занятостью
- ☑ Постройте взаимодействие с бизнес подразделения и службой безопасности