



**ЗАДАЧИ БИЗНЕСА, ДЛЯ  
РЕШЕНИЯ КОТОРЫХ НУЖНО  
DLP. ПРИМЕРЫ ИЗ ПРАКТИКИ  
ВНЕДРЕНИЯ**

---

*«Владея информацией,  
владеешь миром»*



# ОБНАРУЖИТЬ ОТПРАВКУ ДСП ДОКУМЕНТАЦИИ ПО ПОЧТЕ ИЛИ ВЫНОС ДРУГИМ СПОСОБОМ



- **Дано:**
- В организации есть ряд ДСП и других конфиденциальных документов.
- Форматы: MS Office, OpenOffice, pdf, ...
- **Требуется:**
- Обнаружить и предупредить СБ при отправке наружу таких документов



**LanAgent**

«Владея информацией, владеешь миром»



## ОБНАРУЖЕНИЕ ОТПРАВКИ ДСП ДОК-ОВ. РЕШЕНИЕ:



**LanAgent**

«Владея информацией, владеешь миром»

- На компьютеры сотрудников ставим следящие модули DLP LanAgent, на сервер – модуль расширенного поиска. С их помощью:
- 1). сокращаем количество каналов передачи документов наружу:
- Наиболее частые каналы утечек – облачные хранилища (файло-обменники, гугл/яндекс диск, облако майл.ру и т.д.)
- Следующие по частоте - съемные накопители, телефоны, личная почта, корпоративная почта, принтер.
- Ненужные для работы каналы – блокируем (личную почту, файло-обменники, диски, ...).
- 2). Для всех каналов ведем логгирование передачи данных и делаем копии отправленных документов.

Оповещения безопасности | Оповещения продуктивности

**Уведомлять специалиста безопасности при следующих событиях:**

При отправке почты на все адреса кроме домена:   
 Только если есть вложение

При отправке письма через браузер

При копировании файла на USB накопитель при размере файла более:  МБ  
 Только в нерабочее время

Копирование на накопитель файлов за день общим размером более  МБ

При выгрузке файла через браузер при размере файла более:  МБ  
 Только в нерабочее время

Выгрузка файлов за день через браузер общим размером более  МБ

Включение компьютера/вход пользователя в нерабочее время

Печать документов на принтере в нерабочее время

Печать за день на принтере более  документов

Печать за день на принтере более  страниц

Поисковые запросы

Строка поиска

Опции поиска  
 Точное совпадение  
 Толерантный поиск

Все слова должны быть в поиске  
 Расстояние между словами   
 Повторяется в тексте более  раз

Где искать  
 Текст  
 Файлы содержимое

Принтеры  
 Теневое копирование  
 Skype  
 Почта  
 Интернет  
 Док-ты на дисках

Дополнительные параметры  
 Имя файла  
 AND   
 Размер файла, Байт ОТ  ДО   
 Домен почты  
 AND

Сгенерировать запрос

Комментарий:

# ОБНАРУЖЕНИЕ ОТПРАВКИ ДСП ДОК-ОВ. РЕШЕНИЕ:



## LanAgent

«Владея информацией, владеешь миром»

- 3). Автоматизируем обнаружение передачи ДСП документов:
- Составляем правила быстрого реагирования** (по внешним признакам, без разбора содержимого)
- Составляем правила реагирования по содержимому:**
  - словарь ключевых фраз, которые основа конфиденциальных документов.
  - в правилах поиска задаем частоту ключевых фраз в тексте и расстояние между словами, при которых правила должны срабатывать
  - анализ ведется с учетом возможного намеренного искажения – опечаток, подмены букв в тексте и т.д.



- ИТОГО:
- 1). Часть возможных каналов утечки заблокирована
- 2). Для всех каналов контролируется передаваемое содержимое и делается его копия.
- 3). По собранным данным ведется автоматический поиск нарушений. Как по внешним признакам, так и по содержимому
- 4). При сработке правила, происходит уведомление специалиста службы безопасности

## ОБНАРУЖЕНИЕ ОТПРАВКИ ДСП ДОК-ОВ. РЕШЕНИЕ:



**LanAgent**

«Владея информацией, владеешь миром»



## ОБНАРУЖЕНИЕ ОТПРАВКИ ДСП ДОК-ОВ. ПРИМЕР ИЗ ПРАКТИКИ № 1:



**LanAgent**

«Владея информацией, владеешь миром»

- **Завод с конструкторским отделом**
- Необходимо было обнаруживать несанкционированную отправку наружу конструкторской документации.
- - Применены все указанные ранее действия.
- - В качестве словаря для поиска были заданы специальные термины, используемые в документации.



## ОБНАРУЖЕНИЕ ОТПРАВКИ ДСП ДОК-ОВ. ПРИМЕР ИЗ ПРАКТИКИ № 2:



**LanAgent**

«Владея информацией, владеешь миром»

- **Бухгалтерская компания (аутсорсинг)**
- требовалось обнаруживать попытку выноса бухгалтерами или менеджерами по продажам списка клиентов – юр. лиц (баз клиентов)..
- - в качестве ключей для поиска были заданы формы собственности компаний: ООО, АО, ИП, а также реквизиты: ИНН, КПП и т.д.
- - бухгалтерам и продавцам по работе приходится пересылать много документов, содержащих те же ключи (счета, счет-фактуры, договора и т.д.).
- - Чтобы избежать ложные срабатывания, задано пороговое значение количества вхождений, при котором считать, что правило сработало.



# ОБНАРУЖИТЬ НЕСАНКЦИОНИРОВАННОЕ ПОЯВЛЕНИЕ НА ПК СОТРУДНИКОВ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

## Дано:

У организации есть сетевой ресурс с конфиденциальными документами.

Сотрудникам разрешено работать с документами на этом ресурсе, но запрещено копировать документы на свой компьютер.



**LanAgent**

«Владея информацией, владеешь миром»



# ОБНАРУЖИТЬ НЕСАНКЦИОНИРОВАННОЕ ПОЯВЛЕНИЕ НА ПК СОТРУДНИКОВ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

## Решение:

Если запрет на копирование из конфиденциального каталога строгий, то создать в LanAgent специальное правило конфиденциального каталога.

Файлы будут доступны для изменений только в указанном каталоге, попытки скопировать их за пределы каталога будут блокироваться.



**LanAgent**

«Владея информацией, владеешь миром»

# ОБНАРУЖИТЬ НЕСАНКЦИОНИРОВАННОЕ ПОЯВЛЕНИЕ НА ПК СОТРУДНИКОВ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

## Плюсы:

Предотвращает любые попытки выноса конфиденциальной информации. В т.ч. позволяет блокировать копирование фрагментов документов в буфер или печати их на принтер.

## Минус:

Как и любое правило строго запрета, усложняет процесс работы с документами. В ряде случаев, бизнес процесс не позволяет так делать.



**LanAgent**

«Владея информацией, владеешь миром»



**ОБНАРУЖЕНИЕ  
НЕСАНКЦИОНИРОВАННЫХ  
КОНФИДЕНЦИАЛЬНЫХ ДОК-ОВ.  
ПРИМЕР ИЗ ПРАКТИКИ:**



**LanAgent**

«Владея информацией, владеешь миром»

## • **Конструкторская организация**

Работа сотрудников в программе «Компас», но не напрямую, а через специальную среду, сохраняющую историю изменений и дополнительную информацию к чертежам.

### **Необходимо:**

- предотвратить копирование чертежей со служебного ресурса,
- дать возможность работать с чертежами только в специальной среде.

### **Решение:**

Создано правило конфиденциального каталога, позволяющее работать с заданным каталогом определенным сотрудникам и только в специально заданной программе. Для всех остальных сотрудников и всех других программ - создано запрещающее правило.



# ОБНАРУЖИТЬ НЕСАНКЦИОНИРОВАННОЕ ПОЯВЛЕНИЕ ДОКУМЕНТОВ БЕЗ СТРОГО ЗАПРЕТА

## Дано:

Для работы, сотрудникам нужен полный доступ к документам.

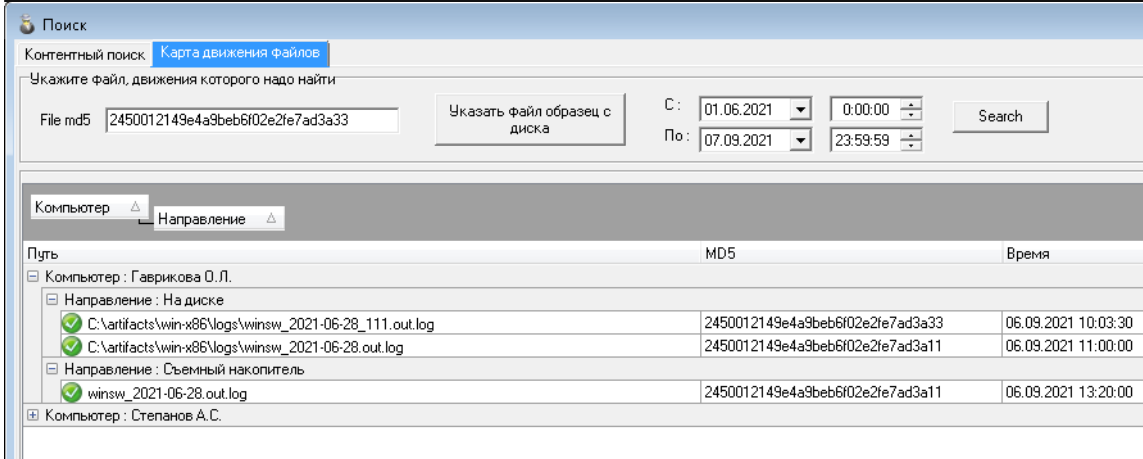
## Требуется:

- уведомлять службу безопасности о несанкционированных копиях документов на рабочих станциях.
- уведомлять о попытках сотрудников отправки или копирования конфиденциальных документов наружу компьютера.



**LanAgent**

«Владея информацией, владеешь миром»



## ОБНАРУЖИТЬ НЕСАНКЦИОНИРОВАННОЕ ПОЯВЛЕНИЕ ДОКУМЕНТОВ БЕЗ СТРОГО ЗАПРЕТА



**LanAgent**

«Владея информацией, владеешь миром»

- **Решение:**
- В LanAgent EnterpriseDLP включена индексация документов на компьютерах сотрудников:
- - служба безопасности в любой момент может просмотреть список документов, которые есть на компьютерах сотрудников, сделать поиск по ключевым фразам в ручном режиме.
- - можно настроить автоматические правила для обнаружения несанкционированных копий при их появлении на ПК сотрудников.
- Можно построить карту движения файла на компьютерах сотрудников: где документ есть, историю изменений и пересылок наружу.



# АВТОМАТИЧЕСКИЙ ТАБЕЛЬ УЧЕТА РАБОЧЕГО ВРЕМЕНИ СОТРУДНИКОВ

В задачи DLP это не входит, но это частый запрос от руководства и отдела по работе с персоналом.

## Требуется:

- подсчет времени работы сотрудников, особенно на удаленке
- выявление нарушений трудовой дисциплины.
- определение продуктивности работы сотрудников



**LanAgent**

«Владея информацией, владеешь миром»

Аналитические отчеты

Суммарный по рабочему времени

Пользователь	Включен	Активность	Простой	% активности	Планир.	Переработка	В выходные	Прогноз
Егорова С.В.	1д. 0ч. 55мин.	13ч. 23мин.	17ч. 22мин.	43	1д. 0ч. 0мин.	-1ч. 48мин.	0ч. 0мин.	0
Захарова Л.С.	1д. 0ч. 46мин.	1д. 3ч. 59мин.	5ч. 47мин.	82	1д. 0ч. 0мин.	1ч. 46мин.	0ч. 0мин.	0
Иванченко А.Б.	22ч. 48мин.	22ч. 29мин.	0ч. 19мин.	99	1д. 0ч. 0мин.	-5ч. 11мин.	0ч. 0мин.	0
Кривошеино И.Г.	1д. 3ч. 14мин.	17ч. 32мин.	9ч. 41мин.	64	1д. 0ч. 0мин.	-4ч. 45мин.	0ч. 0мин.	0
Легуша О.В.	15ч. 18мин.	5ч. 7мин.	7ч. 10мин.	53	1д. 0ч. 0мин.	-16ч. 41мин.	0ч. 0мин.	1
Луцкая А.П.	1д. 10ч. 1мин.	19ч. 16мин.	14ч. 45мин.	56	1д. 0ч. 0мин.	2ч. 1мин.	0ч. 0мин.	0
Ярлова А.З.	1д. 11ч. 6мин.	1д. 10ч. 48мин.	0ч. 18мин.	99	1д. 0ч. 0мин.	3ч. 6мин.	0ч. 0мин.	0

Аналитические отчеты

Табель рабочего времени

Пользователь: Егорова С.В.

Дата	Включен	Активность	Простой	% активности	Начало	Окончание	График	Планир.	Переработка
10.08.2021	7ч. 42мин.	4ч. 56мин.	2ч. 48мин.	64	9:28:19	18:31:11	Рабочий	0ч. 0мин.	0ч. 17мин.
11.08.2021	0ч. 2мин.	2ч. 16мин.	5ч. 50мин.	27	9:43:32	18:30:19	Рабочий	0ч. 0мин.	0ч. 2мин.
12.08.2021	0ч. 8мин.	3ч. 11мин.	4ч. 51мин.	39	9:22:16	18:30:24	Рабочий	0ч. 0мин.	0ч. 8мин.
13.08.2021	7ч. 17мин.	3ч. 17мин.	3ч. 44мин.	47	9:53:36	17:32:30	Рабочий	0ч. 0мин.	0ч. 58мин.

Объединенный отчет время работы ПК и приложений

с: 10.08.2021 по: 13.08.2021 23:59:59

Компьютер	Включен	% активности	Проведено	Microsoft Outlook	Microsoft Excel	Удален	Skype	Microsoft Edge	1cs3	Google Chrome	Прочие
Егорова С.В.	1д. 0ч. 55мин.	43	12%	22%	44%	17%	2%	2%	0	0	1%
Захарова Л.С.	1д. 0ч. 46мин.	82	7%	5%	65%	0	12%	1%	0	4%	6%
Иванченко А.Б.	22ч. 48мин.	98	10%	4%	45%	0	1%	30%	6%	0	5%
Кривошеино И.Г.	1д. 3ч. 14мин.	64	12%	2%	97%	0	2%	5%	6%	7%	8%
Легуша О.В.	15ч. 18мин.	53	14%	0	51%	0	0%	31%	0	0	5%
Луцкая А.П.	1д. 10ч. 1мин.	56	2%	5%	88%	0	0%	0	0	0%	4%
Максимов О.В.	0ч. 0мин.	0	0	0	0	0	0	0	0	0	0
Петрова В.О.	0ч. 0мин.	0	0	0	0	0	0	0	0	0	0
Степанов Д.И.	0ч. 0мин.	0	0	0	0	0	0	0	0	0	0
Ярлова А.З.	1д. 11ч. 6мин.	99	6%	6%	79%	0	8%	4%	0	2%	4%

- Учет рабочего времени – это штатная функция LanAgent

## Решение:

- на компьютерах сотрудников устанавливаем следящий модуль
- задаем график рабочего времени для разных категорий сотрудников
- настраиваем списки продуктивных и непродуктивных программ и сайтов для разных категорий сотрудников.
- определяем график автоматического формирования отчетов по расписанию.
- при необходимости, настраиваем отправку отчетов на почту.

# УЧЕТ РАБОЧЕГО ВРЕМЕНИ. РЕШЕНИЕ:



## LanAgent

«Владея информацией, владеешь миром»

1. Защиту конфиденциальных данных лучше проводить в несколько этапов:
  - Блокировка не нужных для работы каналов передачи данных.
  - Быстрые правила – срабатывающие по внешним признакам.
  - Правила на основе анализа содержимого
2. Когда бизнес-процесс не позволяет вводить для сотрудников строгие ограничения на работу с данными - особенно важно вести контроль всех каналов и сохранять копии передаваемых данных. В этом также поможет DLP система.
3. Кроме возможностей DLP, от системы часто ожидается решение задач бизнеса: учет рабочего времени, контроль соблюдения дисциплины, помощь в организации работы дистанционных сотрудников.



## ВЫВОДЫ



**LanAgent**

«Владея информацией, владеешь миром»





**ООО «Забота»**  
**Бессонов Евгений Владимирович**  
**+79137378825**  
**[bessonov\\_ev5@mail.ru](mailto:bessonov_ev5@mail.ru)**