# 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: МС Офис, OpenOffice, pdf, …
- **Требуется**:
- Обнаружить и предупредить СБ при отправке наружу таких документов

LanAgent

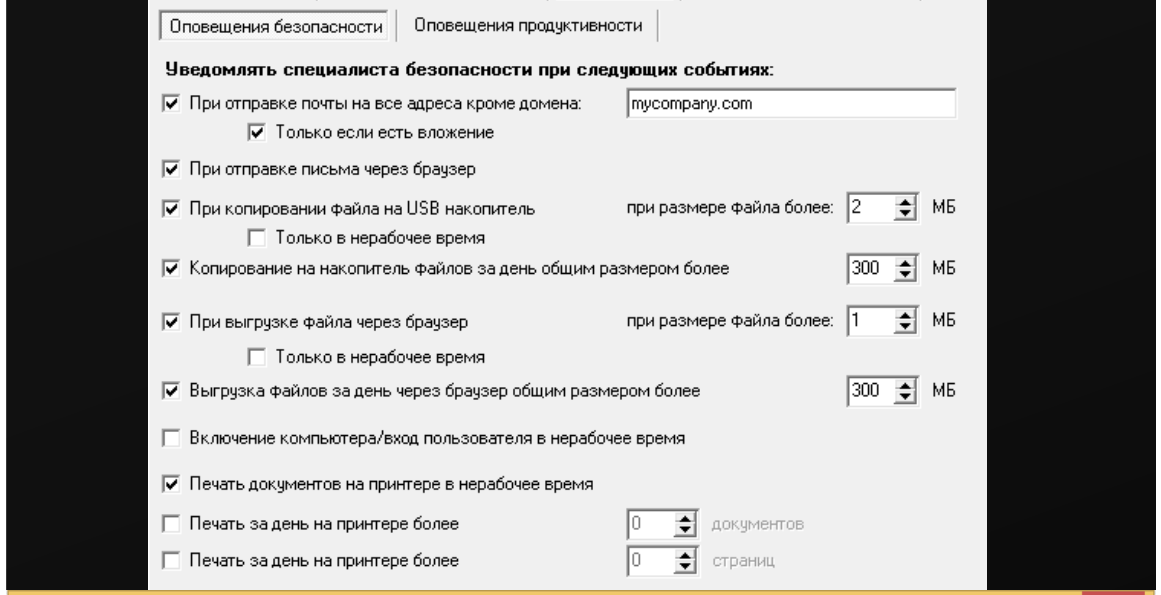
«Владея информацией, владеешь миром»

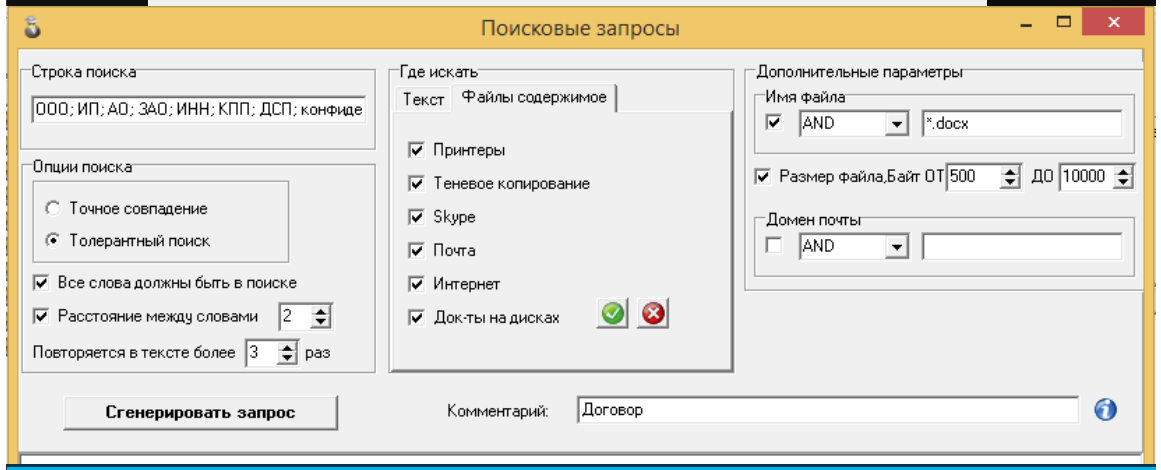
# ОБНАРУЖЕНИЕ ОТПРАВКИ ДСП ДОК-ОВ. РЕШЕНИЕ:

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.




# 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.

# ОБНАРУЖЕНИЕ ОТПРАВКИ ДСП ДОК-ОВ. РЕШЕНИЕ:

LanAgent

«Владея информацией, владеешь миром»

- 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. 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.

LanAgent

«Владея информацией, владеешь миром»

# 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.

# 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»

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.

# 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.

LanAgent

«Владея информацией, владеешь миром»

# ОБНАРУЖИТЬ НЕСАНКЦИОНИРОВАННОЕ ПОЯВЛЕНИЕ ДОКУМЕНТОВ БЕЗ СТРОГО ЗАПРЕТА

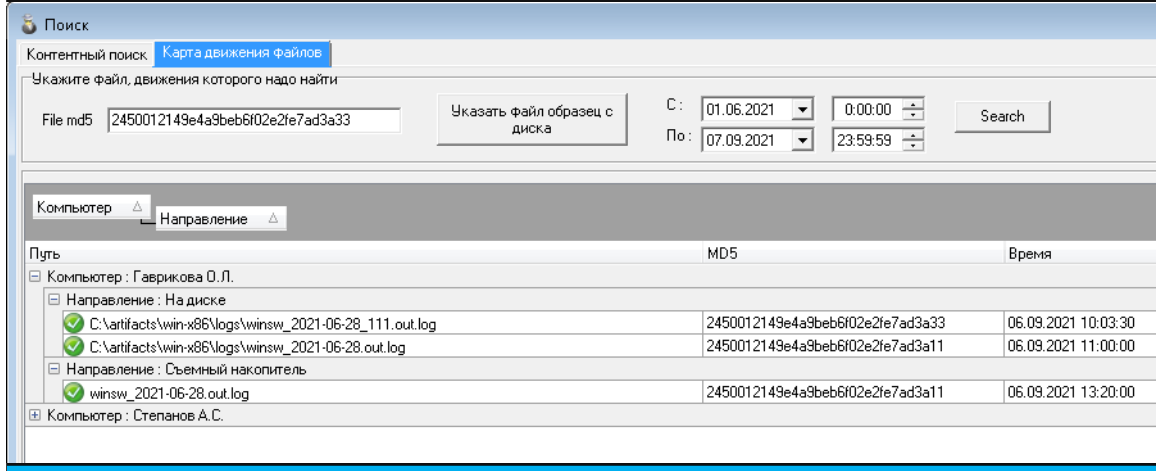
**Дано**:

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.




# 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.

LanAgent

«Владея информацией, владеешь миром»

# АВТОМАТИЧЕСКИЙ ТАБЕЛЬ УЧЕТА РАБОЧЕГО ВРЕМЕНИ СОТРУДНИКОВ

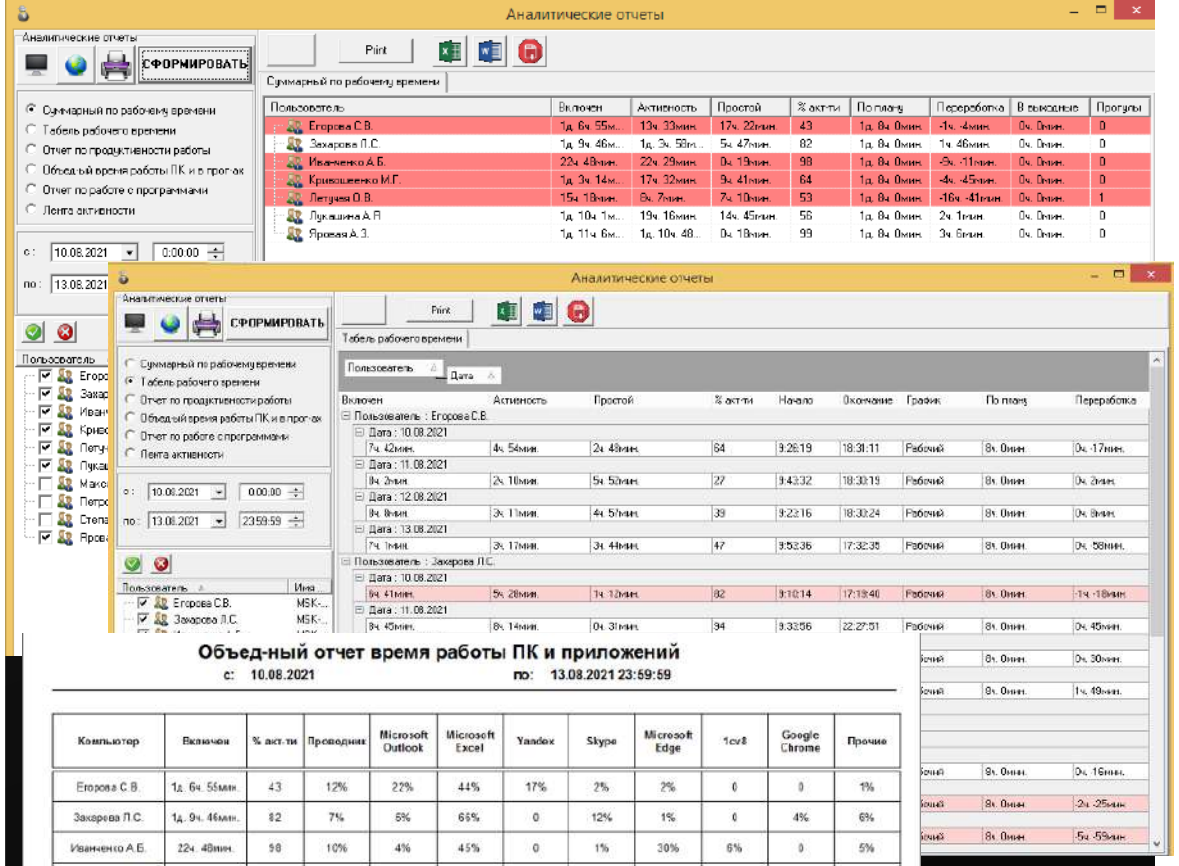
В задачи DLP это не входит, но это частый запрос от руководства и отдела по работе с персоналом.

**Требуется**:

- подсчет времени работы сотрудников, особенно на удаленке

- выявление нарушений трудовой дисциплины.

- определение продуктивности работы сотрудников




# УЧЕТ РАБОЧЕГО ВРЕМЕНИ. РЕШЕНИЕ:

LanAgent

«Владея информацией, владеешь миром»

- 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.

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**