SEARCHINFORM

Шорт-лист задач для DCAP:

с чем не справятся другие СЗИ

Александр Янчук

Заместитель генерального директора
по СЗФО, УрФО, СФО и ДФО

DCAP – СИСТЕМЫ ДЛЯ АУДИТА И ЗАЩИТЫ ДАННЫХ В ПОКОЕ. ЧТО ЭТО ЗНАЧИТ?

В теории (по Gartner):

- Классификация данных.
- Хранение конфиденциальных данных.
- Управление безопасностью данных.
- Мониторинг и аудит данных.
- Защита всех данных от несанкционированного доступа и использования.

SEARCHINFORM

НА ДЕЛЕ: В «СЁРЧИНФОРМ FILEAUDITOR»

Классификация конфиденциальных данных

Находит в общем документообороте файлы, которые содержат критичную информацию, и присваивает каждому метку определенного типа: персональные данные, коммерческая тайна, номера кредитных карт и т.д.

Аудит прав доступа

Облегчает контроль за доступом к уязвимой информации – автоматически отслеживает открытые ресурсы, файлы, доступные конкретному пользователю или группе, учетные записи с привилегированными правами.

Архивирование критичных документов

Делает теневые копии критичных файлов, найденных на ПК, сервере или в сетевых папках и сохраняет историю их редакций. Архив критичных данных помогает в расследованиях инцидентов и гарантирует восстановление потерянной информации.

Контроль и блокировки действий пользователей

Производит аудит пользовательских операций в файловой системе. ИБ-служба всегда в курсе актуальной информации о «жизни» файла (создание, редактирование, перемещение, удаление и т.д.). Блокирует нежелательную активность с файлами в любом произвольном приложении.

ПО СУТИ

SEARCHINFORM

FileAuditor отвечает на важные вопросы внутренней информационной безопасности:

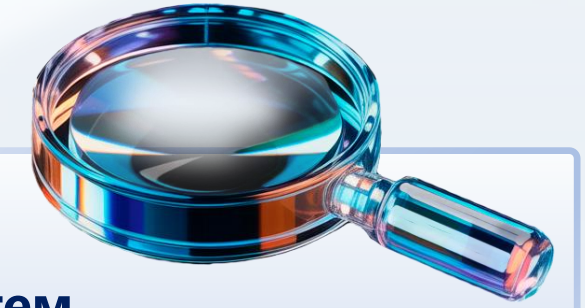
Какие документы содержат критичную для бизнеса информацию?

Сколько в компании таких данных и где они находятся?

Кто имеет к ним доступ и может их редактировать?

И позволяет всем этим управлять.

ЧТО ИСКАТЬ В ПЕРВУЮ ОЧЕРЕДЬ?



- **Персональные данные (152-ФЗ для всех, иначе – «оборотка»)**
- **Информацию из критичных систем**
- **Финансовые данные**
- **Все о клиентах (договоры, клиентские базы, КП)**
- **Коммерческую тайну –** ***задачка со звездочкой****

450+

правил уже готовы «из коробки», достаточно включить

SEARCHINFORM

КАК ОПРЕДЕЛИТЬ, ГДЕ КОМТАЙНА?

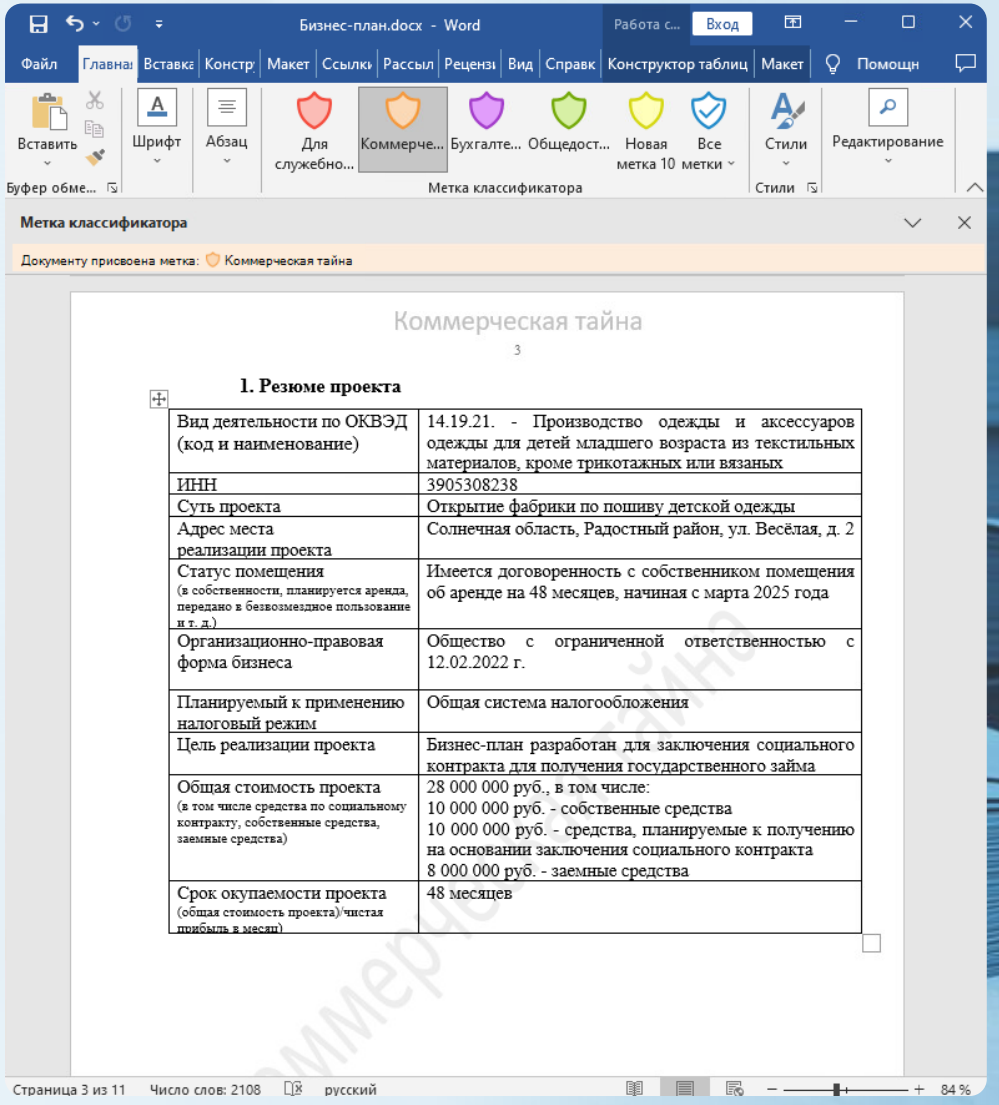
Проблема:

Что относится к КТ – решение конкретных людей.

Решение:

Ручные метки классификации в FileAuditor

- Автор/рецензент документа ставит метку сам
- Уровень конфиденциальности виден сразу – это выполняет требования к обеспечению режима КТ
- Система автоматически перепроверит, верно ли поставили ручную метку



КАК ЗАЩИТИТЬ КРИТИЧНОЕ?

SEARCHINFORM

Ни NAS, ни сетевые папки, ни управление через AD
не используют контент-зависимые признаки
при назначении прав.

Но важны не «все документы PDF»,
а «все договоры с клиентами»!

«Классическое» распределение доступа:

- права по пользователям/группам
- зависит от атрибутов
- не учитывает ценность
- **не исключает риски**

КАК РАБОТАЕТ КОНТЕНТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

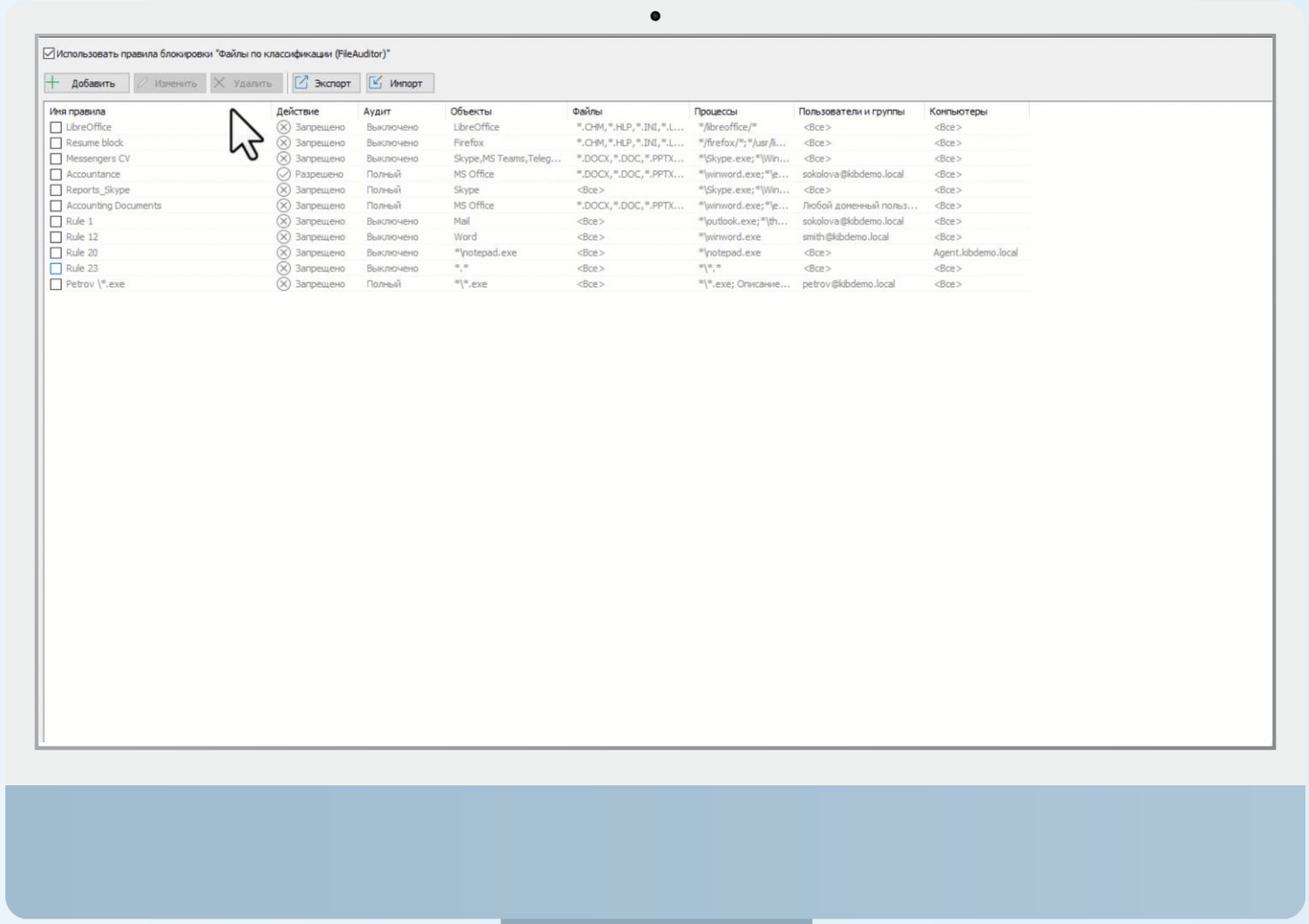
SEARCHINFORM

В FileAuditor:

- Блокировки доступа настраиваются по меткам классификации
- Метка остается на документе, пока в нем есть конфиденциальный контент = блокировка продолжает действовать
- Запрет нежелательных вариантов обработки документа

  Например: нельзя открывать в редакторе, прикреплять в почтовом клиенте/мессенджере и др.

Это работает для *любого* процесса



КОНТРОЛЬ «СЛЕПЫХ ЗОН»

SEARCHINFORM

DCAP – универсальное средство,
чтобы защитить файлы в любом канале,
который не защищен другими СЗИ.

Например:

- Контроль пользовательского ПО и сервисов
- DLP не работает с этим каналом

Вы можете настроить точечную блокировку в FileAuditor:

«в **ЭТОМ** процессе вот **ЭТИ** файлы открыть нельзя».

ЦЕНТРАЛИЗАЦИЯ АУДИТА AD

SEARCHINFORM

Нет единых систем аудита пользовательской активности!

DCAP:

- **Локальные операции**
  через собственный драйвер для разных ОС
- **Права доступа** для всех СХД, ОС и иных хранилищ
- **Журналы Контроллеров домена**
  на случай сетевой работы

Это позволяет применять **ЕДИНЫЕ**
правила аудита для разрозненных систем

СИНХРОНИЗАЦИЯ НАСТРОЕК ДОСТУПА

SEARCHINFORM

Кейс: распределенная инфраструктура

- в локальных хранилищах настройки доступа из AD
- в сетевых папках настройки доступа из NAS
- свои настройки в разных «облаках», БД, критичных системах (например, CRM)

Синхронизировать вручную долго
и не всегда возможно.

DCAP применяет свои настройки
одновременно и одинаково
в любых источниках.

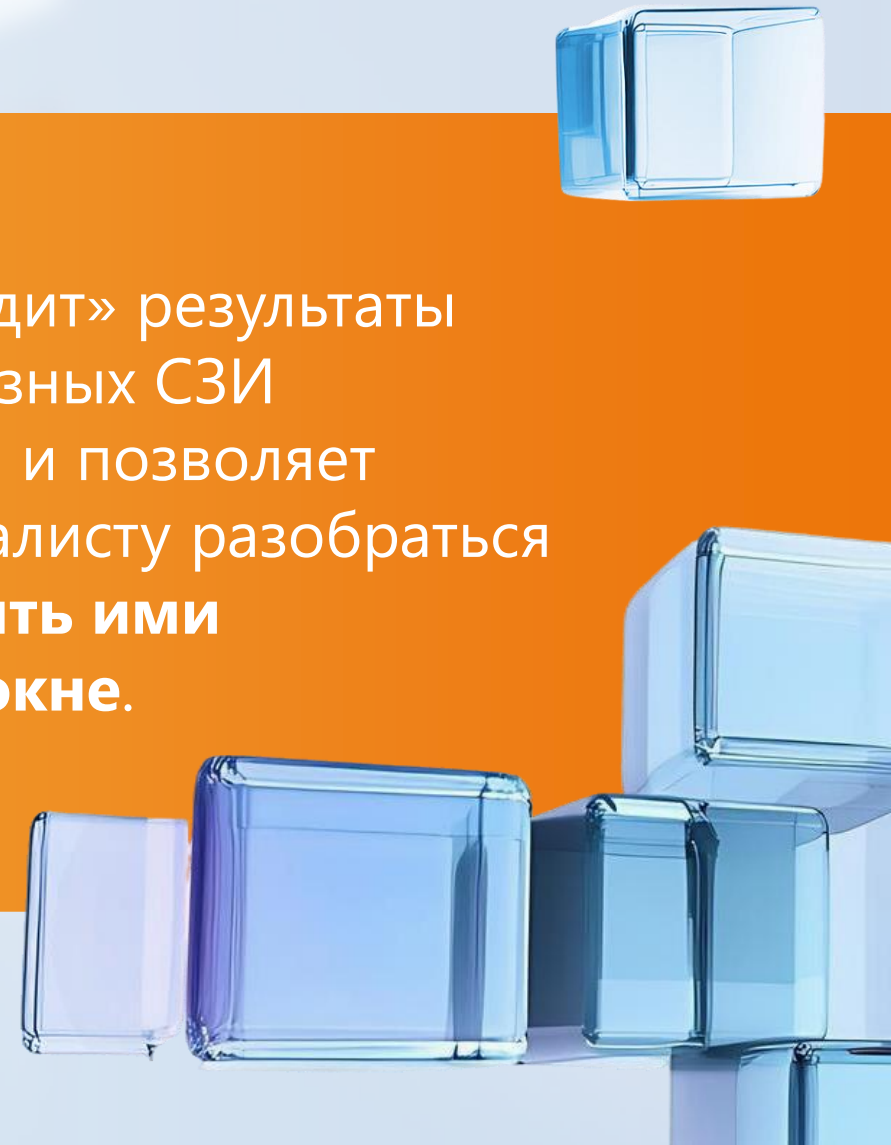
ОБЪЕДИНЕНИЕ СЗИ

SEARCHINFORM

Средства защиты работают с файлами по-разному:

- Антивирусы
- DLP
- Средства классификации (MS Information Protection и др.)
- EveryTag и аналоги
- Средства шифрования

DCAP «видит» результаты работы разных СЗИ с файлами и позволяет ИБ-специалисту разобраться и **управлять ими в одном окне**.



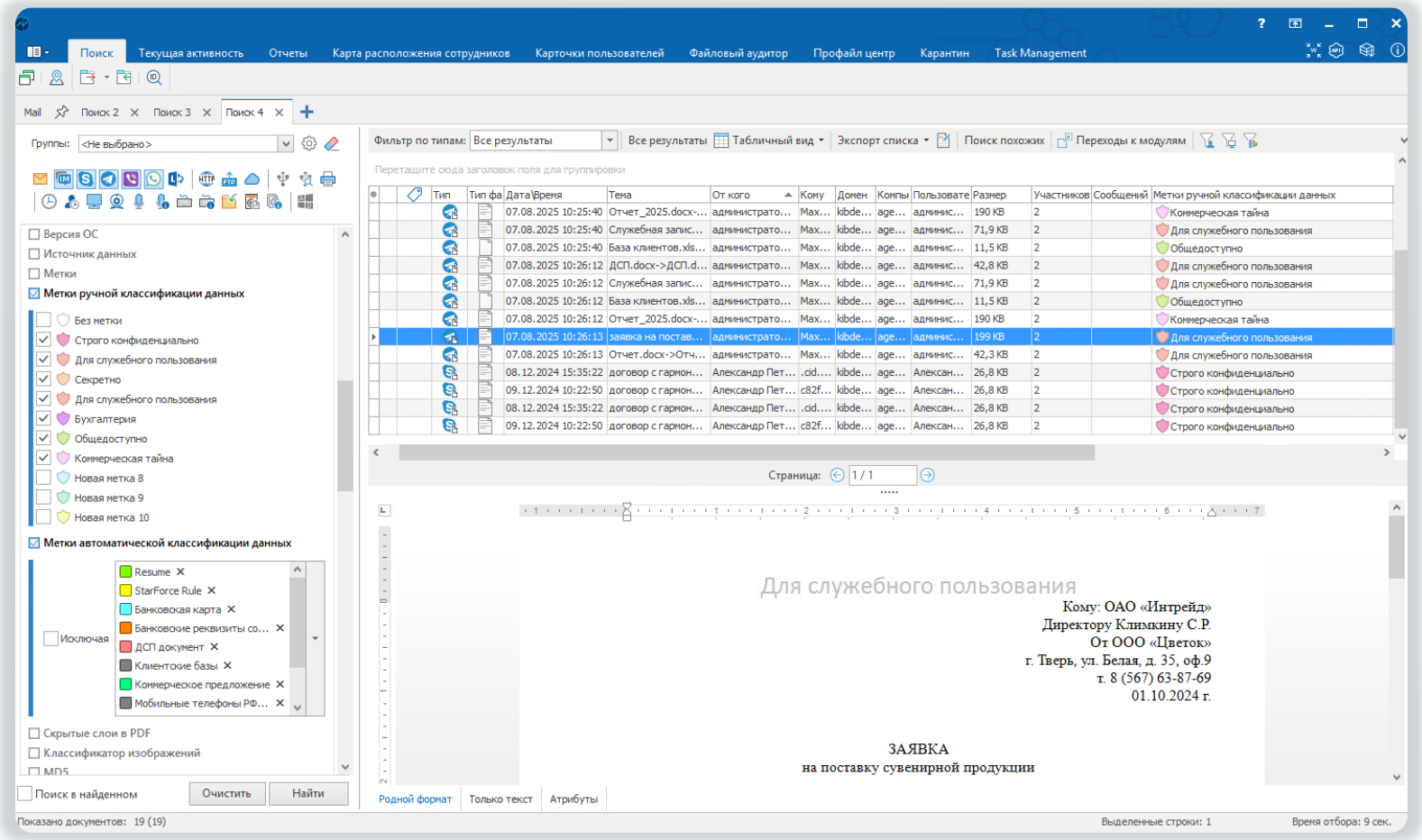
БОНУС: «РАЗГРУЗКА» СЗИ

SEARCHINFORM

DCAP снимает нагрузку с других средств защиты информации за счет ускорения контентного анализа.

Кейс: работа с DLP

- DCAP классифицировал файл по контенту
- DLP не нужно вычитывать файл повторно, чтобы понять, что внутри
- Для сработки политики DLP требуется меньше времени и ресурсов на анализ



УМНЫЙ БЭКАП

SEARCHINFORM

Нет систем бэкапирования, которые работают на основе реальной ценности данных: только по директориям, атрибутам файлов.

DCAP:

- **Сохраняет** теневые копии **критичных документов** на основе контента
- **Защищает** от нежелательных изменений и удалений по вине пользователей
- **Страхует** на случай атаки шифровальщика
- **Экономит** ресурс:
  - можно бэкапировать выборочно – классы и конкретные документы
  - хранится нужное число редакций
  - работает дедупликация

SEARCHINFORM

БОНУС:
ОПТИМИЗАЦИЯ ХРАНЕНИЯ

DCAP анализирует объемы хранения и обращения к данным. С ним можно:

- **Найти «файловый мусор»:**
  неиспользуемые, неактуальные документы и др.
- **Найти дубликаты:**
  нежелательные копии, шаблоны, «ползучие бэкапы», повторные скачивания и др.
- **Составить статистику хранения**
  тяжелых данных (например, медиа), которые не нужны в работе

На основе анализа делаете очистку – высвобождаете дорогое место в СХД.

Как мы сами «разгребали» СХД с FileAuditor

СПАСИБО ЗА ВНИМАНИЕ!

SEARCHINFORM

https://t.me/searchinform

https://vk.com/
securityinform

ПРАКТИКА И АНАЛИТИКА

https://searchinform.ru/
practice-and-analytics/